and Mark Gitsenstein of my staff be accorded the privilege of the floor during the consideration of this measure.

The PRESIDING OFFICER. Without objection, it is so ordered.

Does the Senator from Nebraska wish to renew his unanimous-consent request?

Mr. HRUSKA. I renew my request, Mr. President.

The PRESIDING OFFICER. Without objection, it is so ordered.

INTRODUCTION OF S. 2963 THE CRIMINAL JUSTICE INFORMATION CONTROL AND PROTECTION OF PRIVACY OF 1974

Mr. ERVIN. Mr. President, with Mr. HRUSKA, Mr. MATHIAS, Mr. KENNEDY, Mr. BAYH, Mr. TUNNEY, Mr. YOUNG, Mr. BROOKE, Mr. MANSFIELD, Mr. ROBERT C. BYRD, Mr. BURDICK, Mr. ROTH, Mr. HUGH SCOTT, Mr. THURMOND, and Mr. FONG, I introduce for appropriate reference the "Criminal Justice Information Control and Protection of Privacy Act of 1974." The purposes of this legislation are to impose certain restrictions upon the type of information which can be collected and disseminated by law enforcement agencies on the Federal, State, and local levels; to place limitations upon the interchange of such information both among such agencies and outside the criminal justice community and otherwise to protect the privacy and reputations of persons about whom the agencies have collected information.

This legislation deals with the most prized but also the most perishable of our civil liberties—the right to privacy. Although the bill is limited to the activities of criminal justice agencies, its enactment would represent an important first step in reestablishing a workable balance between the information needs of Government on the one hand and the sanctity, individuality, and privacy of American citizens on the other. To understand the impact on personal privacy and the urgent need for this legislation, let me first review the significance of recordkeeping by law enforcement and other Government agencies.

I. GOVERNMENT RECORDKEEPING AND THE RIGHT TO PRIVACY

During the past few decades the demands by Government for personal and sensitive information about its citizens have escalated. This insatiable appetite for information among Government policymakers and administrators is closely related to the increasing responsibility which we have placed upon government, especially the Federal Government, for our health, safety, and well-being. The Government is expected to manage the most complex economy in history; to collect and expend billions of tax dollars in a productive manner each year; as well as to study and attempt to ameliorate the various crises which seem to plague our country with depressing regularity, involving our environment, energy resources, crime, and so on. Most Americans are willing to cooperate by divulging information about virtually every aspect of their lives if they believe it will help the Government fulfill these responsibilities.

Yet if we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.

Alexander Solzyhenitsyn, the Russian Nobel Prize winner, suggests how an all-knowing government dominates its citizens in his book "Cancer Ward:"

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber, banks, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

Perhaps it should come as no surprise that a Russian can master the words to describe the elusive concept we in America call personal privacy. He understands, in a way which we cannot, the importance of being a free individual with certain inalienable rights, an individual secure in the knowledge that his thoughts and judgments are beyond the reach to the state or any man. He understands those concepts because he has no such security or rights but lives in a country where rights written into law are empty platitudes.

Privacy, like many of the other attributes of freedom, can be easiest appreciated when it no longer exists. A complacent citizenry only becomes outraged about its loss of integrity and individuality when the aggrandizement of power in the Government becomes excessive. By then, it may be too late. We should not have to conjure up 1984 or a Russian-style totalitarianism to justify protecting our liberties against Government encroachment. Nor should we wait until there is such a threat before we address this problem. Protecting against the loss of a little liberty is the best means of safeguarding ourselves against the loss of all our freedom.

The protection of personal privacy is no easy task. It will require foresight and the ability to forecast the possible trends in information technology and the information policies of our Government before they actually take their toll in widespread invasions of the personal privacy of large numbers of indivdual citizens. Congress must act before those new systems are developed, and before they produce widespread abuses. The peculiarity of those new complex technologies is that once they go into operation, it is too late to correct our mistakes or supply our oversight.

Our Founding Fathers had that foresight when they wrote the Bill of Rights. The first, fourth, and fifth amendments are among the most effective bulwarks to personal freedom conceived by the mind of man. Justice Brandeis in his classic dissent in the wiretapping case, *Olmstead* v. *United States*, 277 U.S. 438, 478 (1927), described with unsurpassed eloquence the importance of the right to privacy set out in the Constitution. These words do not go stale from repetition:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognize the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.

Government data collection on individuals is not a brand new phenomenon. The Federal Government has been collecting immense amounts of very sensitive information on individuals for decades. Income tax, social security, and census come to mind immediately. Various surveys by experts, private organizations such as the National Academy of Sciences, and a number of congressional committees have established the fact that the Federal Government stores massive amounts of information about all of us.

Several individual dossier files have received considerable publicity in recent years. For example, the Defense Department has several extensive files of very sensitive information, including dossiers on 1.6 million persons in its industrial security files. In the Justice Department alone, there is at least one civil disturbance file with 22,000 names; a file of approximately 250,000 names in the organized crime section; rap sheets or fingerprint cards on over 20 million individuals in the FBI's identification division files, and records on well over 450,000 persons in the FBI's National Crime Information Center—NCIC; and over 40 million names in the master index of the Immigration and Naturalization Service. The National Driver Register of the National Highway Safety Bureau contains 3,300,000 names. There are 69,000 names in the Secret Service files of persons considered potentially dangerous to the President, and the Secret Service computer contains hundreds of thousands of others.

Many of these records are in manual files as opposed to storage in computerized data banks. However, the trend is toward automation of the files so that information on an individual can be made instantly available to users. The FBI's 20 million fingerprint rap sheets are being automated. A survey which the Subcommittee on Constitutional Rights is conducting reveals that there are over 800 data banks in the Federal Govern-

ment, many of which are automated, containing personal information on American citizens.

These figures and other information which the subcommittee's survey has revealed suggest that a revolution is about to take place within the huge information warehouses of the Federal Government. The revolution is going to be caused by two major developments within the Federal bureaucracy—both resulting from the application of highly sophisticated information technology to the Government's files.

First, with the advent of computers the Government is able to increase by geometric proportions the amount of information it can collect on individuals. Prof. Arthur Miller of the Harvard Law School, in his book "The Assault on Privacy," suggests that it will soon be technically feasible to store a 20-page dossier on every single American on a piece of tape less than 5,000 feet long. At the same time, the new technology permits the Government to reduce to microseconds the amount of time necessary to get access to the information. For example, the NCIC computer is able to locate one of its 450,000 criminal histories on an individual, reproduce it and transmit the file to a remote terminal in California or Florida in less than 5 seconds.

Second, and perhaps even more ominous than the computerization of the information, is the development of nationwide information networks by the Federal and State governments, utilizing telephone and other telecommunications lines. These information networks are designed to increase dramatically the number of people and agencies which can access the computerized data banks operated by the Federal, State, and local governments. When the NCIC computerized criminal history is fully operational, it will be one of the largest data bank-information networks of personal dossiers ever attempted. Eventually, roughly 40,000 State and local police departments will have instantaneous access to computerized files on an estimated 21 million individuals who at some time in their lives have been arrested by State, local, or Federal police. The General Accounting Office estimates that this ambitious project may cost over $100,000,000 in Federal, State, and local revenues. Already LEAA's allocations over the past 4 years is estimated at $50 million, not counting State and local expenditures.

The NCIC system is not the first of these systems nor will it necessarily be the largest. As Eugene Levin, an expert on data bank-information networks has pointed out, the Department of Defense has done the pioneering work in this area. The Advanced Research Projects Agency of the Department of Defense has implemented a network which ties together many huge and dissimilar scientific computers. However, the difference between NCIC and the types of systems pioneered by Defense is that the former has sensitive personal information on individuals while the latter is designed to facilitate the transfer of innocuous scientific information.

Mr. Levin suggests the dangers that this new computer-communications technology will have upon our lives once Government begins to use it to collect and disseminate information on individuals:

> The greatest deterrent to extensive government surveillance of individuals has not been the lack of technology of "bugging," nor do considerations of legality, morality, or ethics seem to carry much weight. The deterrent has been "data pollution," which buries an investigator under bits and bytes. It has not been possible to handle (gather, filter, store, process, retrieve, format, disseminate) the huge volume of information on all individuals in anything approaching a useful time frame. *Now it can be done.*

If traditional Government recordkeeping practices and records policies have not yet posed an intolerable threat to personal privacy or reputations, it is only because of the benign inefficiency of these file-drawer record systems. Until very recently, significant amounts of information were not collected about individuals and therefore were not available to others. Use of information collected and kept on a decentralized basis is slow, inefficient, and frustrating. It requires an immense effort to collect information on a specific individual from a variety of different agencies, and then to have it sent out to the agency requesting it. It is ironic but true that what has thus far saved much of our privacy and our liberty has been the complacency, inefficiency, and intraagency jealousies of the Government and its personnel.

This decentralization, of course, is being radically changed by computerization and remote access through data networks. The information in Government files is often rather superficial and general and, in large part, dated and useless. The new technology allows for the collection of much more information on individuals as well as for systematic updating. With computerization and automatic remote access, the Government's ability to collect information increases astronomically and its capacity to broadcast what it ingests to every part of the Nation increases at the same rate. Once an individual gives up information about himself to the Government, he, and in most cases the Government, loses control over it. The citizen cannot, and the Government usually does not, control who can see the information. Nor can he or the Government insure the accuracy of what is broadcast. Increasingly, these systems will influence, if not determine, whether an individual will get Government benefits, be extended credit, get a job, or be considered a criminal and be harassed by police.

II. CRIMINAL JUSTICE DATA BANKS: A MICROCOSM

Over the past few years the Subcommittee on Constitutional Rights, which I chair, has been studying the impact of Government computerized networks and recordkeeping of personal information in the hope of developing legislation to reverse these trends. In the course of this effort, I have come to the conclusion that the need for legislative action respecting criminal justice data banks cannot wait for the development of a comprehensive legislative solution which applies generally to all Government data collection. Therefore, I have drafted legislation which deals with this area in the hope that the experience of developing and enacting this legislation will provide guidance in formulating a more complete Government policy on privacy.

The question of Government collection and dissemination of criminal records and other routine law enforcement information must be the first target for data bank privacy legislation. If Congress can successfully develop privacy safeguards for law enforcement information, collection and dissemination, then our experience may make easier the establishment of a more comprehensive policy. Some of the most advanced technology is being used in local, State, and Federal criminal justice data banks. The type of information being collected in such systems is as sensitive as any collected by Federal or State governments. The complexity of the questions of granting or denying access to subjects and other individuals are as difficult as those involved in any other area of government recordkeeping. I hope that Congress consideration of the "Criminal Justice Information Control and Protection of Privacy Act of 1974" will be the first step in its effort to come to grips on a national level with the assault on privacy by governments and private enterprise wherever it may exist.

Criminal recordkeeping has a long history. Since the 1920's the FBI has been providing a nationwide manual exchange of arrest records for State and local police departments. The purpose of this system is to supplement the files of State and local police departments by making available the arrest record of any person ever arrested for a crime by any police agency. The police utilize these records, called rap sheets, for investigative purposes, even though many of the records never indicate whether the subject has ever been prosecuted, much less convicted, of the crime for which he was arrested.

To my mind, a record of an arrest without any indication of a disposition of the charges arising out of that arrest is virtually useless for law enforcement purposes, and is highly prejudicial if used for non-law enforcement purposes. Yet I understand that in several states as many as 70 percent of the records do not contain dispositions. I would not be surprised to find that the percentage of incomplete records is ever higher in FBI files since those files are based on State files and the FBI depends upon States and localities for record updating.

A record which shows a disposition of no prosecution, dropped charges, or acquittal may have more value, but it is also highly prejudicial if controls on its dissemination do not exist. The number of such records in Federal, State, and local files is significant. In 1972 there were 8.7 million arrests in the United States. Of those 8.7 million arrests, about 1.7 million were for what the FBI terms serious offenses—homicide, rape, robbery, assault, and so forth. According to the FBI, almost 20 percent of the adults arrested for these serious offenses are never even prosecuted, and of those prosecuted, approximately 30 percent are not convicted. For juvenile arrests and arrests

for the 7 million less serious crimes, the percentage of no prosecutions and no convictions is much higher. This suggests that there are probably several million so-called criminal records on persons who were never prosecuted or convicted of the charge for which they were arrested, but which are added to the FBI files each year and available for distribution to any local police department, State civil service commissions, and certain private concerns.

The rap sheet distribution system by the Identification Division of the FBI operates without formal rules. Custom and several letters from the Director of the FBI to local police departments seem to be the only limitation on access to the information. The rap sheets are made available to government licensing agencies, government personnel departments, and, in all too many cases, either directly or indirectly to private employers. By 1973 the magnitude of the dissemination was immense. Each day the Identification Division receives over 11,000 requests for record searches, a large portion of which are from non-law-enforcement agencies.

Unfortunately, when an employer obtains this so-called criminal record information, he is not so concerned with whether the arrest contains disposition of charges or whether the subject was convicted. As far as most employers are concerned, the subject of such a record is a "criminal" and his application is automatically rejected. One survey of New York City employment agencies found that 75 percent would not accept for referral an applicant with an arrest record, whether or not he was convicted. Although the Bureau discourages dissemination of rap sheets to private enterprise for employment purposes, once the information is in the hands of local police, it is effectively out of the control of the Bureau. For example, a few months ago a grand jury in Massachusetts began hearing evidence that State police officers were selling police records to department stores and other private businesses and credit agencies. This unfortunate abuse continues in case after case.

The FBI sends rap sheets to State and municipal civil service commissions as a matter of course. One study found that most state, local and municipal employers consider an arrest record, even one short of a conviction, in determining employment eligibility. As many as 20 percent of these Government employees automatically disqualify someone with an arrest record regardless of the disposition on the record. When you consider these employment policies in light of the fact that the FBI may have rap sheets on almost 10 percent of the population and the fact that Federal, State, and local government employment totals 18 percent of the work force, the impact of this dissemination should be obvious. The FBI does not now have the necessary authority and tools to deal with these and other problems. One purpose of this legislation is to supply the legislative authority that so far is absent.

In 1970, the Law Enforcement Assistance Administration funded a prototype computerized network for sharing criminal offender records. The experiment, called Project SEARCH—system for the electronic analysis and retrieval of criminal histories—took place in the summer of 1970 and demonstrated to the satisfaction of the Justice Department the feasibility of a nationwide computerized network for the exchange of such information. In December of 1970 Attorney General Mitchell authorized the FBI to assume operation of the project SEARCH computerized criminal history—CH—project. The Bureau transferred the CH file to its National Crime Information Center—NCIC—where it already had operational computerized files on stolen securities and persons with outstanding arrest warrants interfaced with a nationwide telecommunications network. The Bureau's ultimate plan is to convert rap sheets received after January 1970 to the CCH file and to also enter into the NCIC/CH file arrests made by any state, local or federal police office. By 1984 there will be some 8 million records on American citizens contained in NCIC and instantly available to approximately 40,000 local police departments.

The law enforcement community is aware of the dangers inherent in collection and dissemination of criminal history information. According to a recent Justice Department report:

> The potential for misusing a criminal record has been amply demonstrated in court cases involving nonautomated records, particularly affecting employment eligibility. Thoughtful law enforcement officials recognize the danger which comes with automation and the interstate exchange of records. The potential problems arising from disclosure, whether authorized or not, are increased many times over those existing in the manual systems.
>
> Most modern law enforcement officials seriously desire to protect the individual's reasonable right to privacy, particularly in those cases where inclusion in the file may have been a mistake or an unjustified result of the formality of criminal justice processes.

Both Project SEARCH and NCIC have made good faith efforts to develop privacy and security guidelines for the operation of their computerized criminal history files. Project SEARCH created a special committee on privacy and security. Their original Privacy and Security Report, Technical report No. 2—popularly called "Tech 2"—was the first comprehensive proposal for adopting privacy rules to the operation of computerized record systems. This bill, and indeed, most other legislation, can trace its antecedents to this original work. NCIC also established a policy advisory committee for its CCH file soon after it took over operation of the SEARCH/CCH file. That group has drafted informal privacy and security guidelines which are revised periodically and do deal with some of the more difficult issues. However, the regulations are largely hortatory. They place most of the security responsibilities on the local data banks which plug into NCIC and do not provide effective enforcement mechanisms. In all fairness, the Bureau cannot be blamed for these inadequacies. It no doubt feels that without special Federal legislation, it lacks the authority to require State and local users to comply with Federal standards on use and collection of criminal justice information. In any case, the most effective remedies, both civil and criminal, must be firmly based in Federal statutory law. Director Kelley recognizes that and has called for Federal legislation which would replace and supplement the informal guidelines pursuant to which NCIC is presently operated. Both Attorney General Saxbe and his predecessor Attorney General Richardson have recognized the need for legislative action, and have taken the lead in developing administration policy in this area.

III. PRIVACY LEGISLATION ON CRIMINAL JUSTICE DATA BANKS

In preparing legislation on this topic I have been influenced greatly by the writings of Prof. Alan Westin of Columbia Law School and Arthur Miller of Harvard Law School, two of the Nation's experts on data banks and privacy. Also, much credit must be given to the HEW Advisory Committee on Automated Personal Data Systems. I have attempted to draft legislation which comports with the recent report of the National Advisory Committee on Criminal Justice Standards and Goals. This Justice Department Commission sets out four basic "potential hazards to the right of privacy" which any privacy legislation relating to criminal justice data banks must address:

> Certainly, privacy can become seriously damaged when the information contained in the national system is (a) inaccurate, (b) incomplete, (c) unjustified, or (d) improperly disseminated.

All of the privacy standards proposed by the Commission, and all of the provisions of the legislation which I am introducing today are addressed to these potential hazards.

The Advisory Commission placed a high priority in reducing, if not eliminating, the amount of inaccurate information in criminal justice information systems. In the Commission's words:

> Joseph A. Burns, 28, of Magnolia Street could have his entire life seriously harmed because of an unwitting confusion between him and Joseph A. Burns of Cass Avenue or Joseph A. Burns, 19, of no known address.

It proposes several standards to govern the quality of information allowed into criminal justice information systems, and access by data subjects for the purpose of review and challenge of their own records. The Commission also takes a strong position against the distribution of incomplete data, such as a record of an arrest with no indication of the disposition of the charges arising out of that arrest. The recommendations oppose the inclusion of any intelligence information in such systems. According to the Commission:

> The criminal justice information system should not supply any information such as the fact that Mr. A was refused entry across the Canadian border in 1970 for lack of sufficient funds, that Mr. A was identified twice in 1969 by police photo-intelligence personnel in the company of leaders of a peace demonstration, or that Mr. A. was a passenger in a car that was stopped and searched—and was permitted to proceed—by New Jersey authorities in 1969. Even

though such information might exist in police intelligence files—and the Commission takes no position here on whether it should—it has no place in the criminal justice information system.

In my judgment, this is one of the most important issues, and my legislation fully endorses this position.

The report proposes a number of enforcement mechanism to insure that its standards are obeyed. It recommends civil and criminal sanctions, the creation of state regulatory commissions and mandatory system audits to insure compliance. My legislation contains similar provisions.

The most difficult question with which the Commission deals and which is also addressed in my legislation, is the question of who shall have access to information contained in criminal justice data banks. In particular, should criminal justice information be made available to noncriminal justice agencies? The Commission answers that question as follows:

Easy availability of criminal justice information files for credit checks, pre-employment investigations, and other noncriminal justice activities is highly prejudicial to the operation of a secure information system designed only for law enforcement agencies.

I heartily agree and my legislation reflects that position.

IV. THE CRIMINAL JUSTICE INFORMATION CONTROL AND PROTECTION OF PRIVACY ACT OF 1974

The Criminal Justice Information Control and Protection of Privacy Act of 1974 is intended to provide a basis for discussion and hearings. It does not pretend to be a final statement on the subject. However, the bill is quite detailed and attempts a resolution of all the major privacy and security issues which have arisen in the development of law enforcement data banks. It endeavors to balance the legitimate needs of law enforcement with the requirements of individual liberty and privacy. It would for the first time give firm statutory authority for criminal justice data banks, a major obstacle in the development of such systems. It would impose upon the data banks strict but manageable privacy limitations. Not the least important, the bill also attempts to solve fundamentally important questions of Federal-State relationships in these comprehensive national information systems.

The bill is divided into three titles. The first title sets out the definitions of 19 terms used in the act. The second title sets out general statutory rules for the collection and dissemination of routine information as well as the more sensitive intelligence information. In the most controversial areas this title sets out specific legislative solutions. For example, there is a complete ban on non-criminal justice use of incomplete information such as raw arrest records. In certain areas, such as right of access, this title sets out general rules but leaves discretion to the States and localities. The third title of the act establishes a joint Federal-State administrative structure for enforcement of the act and for actual operation of interstate criminal justice data banks such as NCIC. This title also requires the States to establish a similar administrative structure for intrastate computer systems.

The highlights of the bill are as follows:

Scope.—The bill would reach criminal justice data banks operated by Federal, State, or local governments. Comprehensive legislation must reach every possible component of the complex interstate data bank network which has grown up in the past decade. Congress cannot depend solely upon internal State legislative action because no one State can effectively regulate what happens to arrest records, and other criminal justice information or intelligence information which finds its way into a data bank in another State. The fact that these systems use interstate communications facilities, are connected with other State systems, or joined with interstate and Federal networks provides, together with the widespread Federal financial support, the necessary constitutional nexus for the legislation.

Focus.—The bill is directed primarily and in the greatest detail at those types of records which have been abused the most—arrest records and so-called "criminal history" records. With regard to records where there are few reported cases of abuse, such as identification records, wanted records or outstanding warrant records, the legislation is much more flexible. In the case of intelligence records, where the potential for abuse is great, the legislation bars computerized information systems. I expect that in the course of hearings on this legislation technical problems will be raised with the specific language used for arrest and criminal history records; that abuses of identification records will be identified; and that law enforcement agencies may make a case for specific exceptions to the ban on computerization of intelligence information or propose concrete suggestions for the regulation of these systems in lieu of an outright prohibition on computerization. One purpose of this bill is to serve as a basis for hearings and discussion on the privacy and data banks controversy.

General dissemination rules: The bill adopts the position of the Senate in its twice unanimously adopted Bible-Ervin rider to recent Justice Department appropriation bills and permits only complete conviction records to be distributed to private employers and other non-law-enforcement users. Here again the bill opts in favor of limited dissemination in the case of records which have an established history of abuse—incomplete arrest and criminal history records. On the question of exchange between law enforcement agencies, the bill adopts a position similar to that of the National Advisory Commission. Generally, only conviction records could be exchanged between police departments. A criminal history record or even a raw arrest record could be given to another department only after the requesting agency had rearrested the subject. It may be the hearings will suggest other limited instances in which raw arrest records can be used.

Updating.—Operators of criminal justice data banks would have to keep all of their records as up to date as in technically feasible and records would have to be accurate. Each data bank must also keep logs reflecting those to whom raw arrest records and certain other sensitive information is sent so that incomplete, inaccurate, or challenged records can be tracked down and corrected or destroyed. The purpose of these provisions is to create an accounting system for information which is permitted to enter and circulate in the data bank network. Strict rules on collection and dissemination are unenforceable if there is no method for keeping track of information flow and meaningless without a requirement that information be as accurate and up to date as possible.

Right of access.—The bill provides every citizen with a right to access any data bank, whether computerized or not, for the purpose of challenge and correction. The challenge procedure includes a hearing before the supervisory personnel of the data bank and if necessary, an appeal to a U.S. District Court. Every significant piece of privacy legislation, including the two administration arrest records bills introduced in the last Congress, contain a citizen access provision similar to the one proposed in this bill.

Civil and criminal penalties.—Operators of data banks will be held criminally and civilly liable for violations of the act. Liability will arise where there is negligence as well as willfullness. Liquidated damages of $100 for each violation would be available, plus complete recovery for all actual and general damages, and where appropriate, exemplary damages, litigation costs and attorneys' fees. This legislation will only command respect if operating personnel and their agencies are held civilly liable for their negligent failure to comply with the letter of each provision.

Administrative provisions.—The bill would create a new independent Federal-State cooperative agency to oversee enforcement of the act. The agency will issue regulations, go to court to enjoin violations and actually take over policy control of the Federal interstate criminal history data bank (NCIC). The purpose of these provisions is to create an agency, which is outside the present law enforcement community and without vested interests in present law enforcement data banks, to administer the act. These provisions of the bill also would give the States their proper role in the development of policy. Representatives of each State will share in the formulation of regulations issued pursuant to the act.

These administrative provisions reflect the concern expressed by many representatives of State and local law enforcement agencies that legislation not delegate great powers to the Federal Government and thereby subordinate the States in the operation of a law-enforcement responsibility that is properly theirs. While none of us in Congress or in the Federal Government desire to see a Federal police force, we must recognize that Federal involvement inevitably leads to Federal control. We must be alert to this even if we have been a little lax in other areas over the

years. Total Federal control over the information systems of State and local police forces is one sure path to a federalized police system in fact if not in name. It might be best to return to the original LEAA plan for project SEARCH. That was a State-controlled, State-operated interstate system, with the Federal Government playing a limited role in providing financing and research. If that is not possible, then the next best approach is a true Federal-State arrangement such as I have proposed in this bill. This is one area where the President's ideal of a New Federalism ought to take concrete form. Since I expect that the States will welcome a return to greater State responsibility and the idea does conform to the New Federalism idea, I have great hopes of a general agreement on this important aspect of the bill.

System audits.—The bill provides for audits of practices and procedures of criminal justice data banks on a random basis by the new independent Federal-State agency and by the States themselves. Most privacy experts agree that systematic audits by outside agencies is a necessary adjunct to civil remedies and citizen rights of access and challenge for enforcement of effective legislation. As long as data bank operators realize that they are subject to random audit by independent computer experts, they are unlikely to ignore the restrictions set out in the act.

V. CONCLUSION

In conclusion, I would like to reaffirm my earlier statement that this legislation is introduced to provoke discussion and to serve as the basis of hearings. Neither I, nor any of the cosponsors feel wedded to all of the provisions of the bill. The Justice Department has been working on similar legislation for the past several months. The President described this legislation in his state of the Union address. I understand that the administration's bill is quite similar in approach to my own, though there are significant technical differences of the two bills. I welcome the administration's effort in this regard and I firmly believe that this issue is both of sufficient national importance and is of such technical complexity that a bipartisan approach is absolutely necessary. In this spirit, I am announcing today hearings before the Subcommittee on Constitutional Rights, which has jurisdiction over this subject, for the purpose of a complete and objective review of both proposals. I consider both my proposal and the Justice Department's forthcoming proposal of equal interest to the subcommittee. I hope that through the hearings which will begin in the near future, we can work out a consensus both within the subcommittee and with the administration so that privacy legislation relating to criminal justice data banks can be enacted before the end of the Congress.

I ask unanimous consent that the bill, a section-by-section analysis of the bill, two columns written by William Safire and Tom Wicker from the New York Times, an editorial in the Washington Post, calling for Federal legislation on this question, be reprinted at this point in the CONGRESSIONAL RECORD.

The PRESIDING OFFICER. The bill will be received and appropriately referred; and without objection, the bill and the material will be printed in the RECORD, as requested.

S. 2963

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Criminal Justice Information Control and Protection of Privacy Act of 1974".

TITLE I—FINDINGS AND DECLARATION OF POLICY; DEFINITIONS

CONGRESSIONAL FINDINGS AND DECLARATION POLICY

SEC. 101. The Congress finds and declares that the several States and the United States have established criminal justice information systems which have the capability of transmitting and exchanging criminal justice information between or among each of the several States and the United States; that the exchange of this information by Federal agencies is not clearly authorized by existing law; that the exchange of this information has great potential for increasing the capability of criminal justice agencies to prevent and control crime; that the exchange of inaccurate or incomplete records of such information can do irreparable injury to the American citizens who are the subjects of the records; that the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from misuse of these systems; that citizens' opportunities to secure employment and credit and their right to due process, privacy, and other legal protections are endangered by misuse of these systems; that in order to secure the constitutional rights guaranteed by the first amendment, fourth amendment, fifth amendment, sixth amendment, ninth amendment, and fourteenth amendment, uniform Federal legislation is necessary to govern these systems; that these systems are federally funded, that they contain information obtained from Federal sources or by means of Federal funds, or are otherwise supported by the Federal Government; that they utilize interstate facilities of communication and otherwise affect commerce between the States; that the great diversity of statutes, rules, and regulations among the State and Federal systems require uniform Federal legislation; and that in order to insure the security of criminal justice information systems, and to protect the privacy of individuals named in such systems, it is necessary and proper for the Congress to regulate the exchange of such information.

DEFINITIONS

SEC. 102. For the purposes of this Act—

(1) "Information system" means a system, whether automated or manual, operated or leased by Federal, regional, State, or local government or governments, including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of information.

(2) "Criminal justice information system" means an information system for the collection, processing, preservation, or dissemination of criminal justice information.

(3) "Criminal justice intelligence information system" means an information system for the collection, processing, preservation, or dissemination of criminal justice intelligence information.

(4) "Automated system" means an information system that utilizes electronic computers, central information storage facilities, telecommunications lines, or other automatic data processing equipment used wholly or in part for data collection, analysis, or dissemination as distinguished from a system in which such activities are performed manually.

(5) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pendng due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, deceased, deferred disposition, dismissed civil action, extradited, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, or executive clemency.

(6) "Dissemination" means the transmission of information, whether orally or in writing.

(7) "Criminal justice information" means information on individuals collected or disseminated, as a result of arrest, detention, or the initiation of criminal proceeding, by criminal justice agencies, including arrest record information, correctional and release information, criminal history record information, conviction record information, identification record information, and wanted persons record information. The term shall not include statistical or analytical records or reports, in which individuals are not identified and from which their identities are not ascertainable. The term shall not include criminal justice intelligence information.

(8) "Arrest record information" means information concerning the arrest, detention, or commencement of criminal proceedings on an individual which does not include the disposition of the charge arising out of that arrest, detention, or proceeding.

(9) "Correctional and release information" means information on an individual compiled by a criminal justice or noncriminal justice agency in connection with bail, pretrial or posttrial release proceedings, reports on the mental condition of an alleged offender, reports on presentence investigations, reports on inmates in correctional institutions or participants in rehabilitation programs, and probation and parole reports.

(10) "Criminal history record information" means information disclosing both that an individual has been arrested or detained or that criminal proceedings have been commenced against an individual and that there has been a disposition of the criminal charge arising from that arrest, detention, or commencement of proceedings. Criminal history record information shall disclose whether such disposition has been disturbed, amended, supplemented, reduced, or repealed by further proceedings, appeal, collateral attack, or otherwise.

(11) "Conviction record information" means information disclosing that a person has pleaded guilty or nolo contendere to or was convicted on any criminal offense in a court of justice, sentencing information, and whether such plea or judgment has been modified.

(12) "Identification record information" means fingerprint classifications, voice prints, photographs, and other physical descriptive data concerning an individual which does not include any indication or suggestion that the individual has at any time been suspected of or charged with criminal activity.

(13) "Wanted persons record information" means identification record information on an individual against whom there is an out-

standing arrest warrant including the charge for which the warrant was issued and information relevant to the individual's danger to the community and such other information that would facilitate the regaining of the custody of the individual.

(14) "Criminal justice intelligence information" means information on an individual on matters pertaining to the administration of criminal justice, other than criminal justice information, which is indexed under an individual's name or which is retrievable by reference to identifiable individuals by name or otherwise. This term shall not include information on criminal justice agency personnel, or information on lawyers, victims, witnesses, or jurors collected in connection with a case in which they were involved.

(15) "The administration of criminal justice" means any activity by a governmental agency directly involving the apprehension, detention, pretrial release, posttrial release, prosecution, defense adjudication, or rehabilitation of accused persons or criminal offenders or the collection, storage, dissemination, or usage of criminal justice information.

(16) "Criminal justice agency" means a court sitting in criminal session or a governmental agency created by statute or any subunit thereof created by statute, which performs as its principal function, as expressly authorized by statute, the administration of criminal justice. Any provision of this Act which relates to the activities of a criminal justice agency also relates to any information system under its management control or any such system which disseminates information to or collects information from that agency.

(17) "Purge" means to remove information from the records of a criminal justice agency or a criminal justice information system so that there is no trace of information removed and no indication that such information was removed.

(18) "Seal" means to close a record possessed by a criminal justice agency or a criminal justice information system so that the information contained in the record is available only (a) in connection with research pursuant to section 201(d), (b) in connection with review pursuant to section 207 by the individual or his attorney, (c) in connection with an audit pursuant to section 206, or (d) on the basis of a court order pursuant to section 205.

(19) "Judge of competent jurisdiction" means (a) a judge of a United States district court or a United States court of appeals; (b) a Justice of the Supreme Court of the United States; and (c) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing access to criminal justice information.

(20) "Attorney General" means the Attorney General of the United States.

(21) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

TITLE II—COLLECTION AND DISSEMINATION OF CRIMINAL JUSTICE INFORMATION AND CRIMINAL JUSTICE INTELLIGENCE INFORMATION

DISSEMINATION, ACCESS, AND USE—GENERALLY

SEC. 201. (a) Criminal justice information may be maintained or disseminated, by compulsory process or otherwise, outside the criminal justice agency which collected such information, only as provided in this Act.

(b) Criminal justice information may be collected only by or disseminated only to officers and employees of criminal justice agencies: *Provided, however,* That beginning two years after enactment of this Act such information may be collected only by or disseminated only to officers and employees of criminal justice agencies which are expressly authorized to receive such information by Federal or State statute. Criminal justice information shall be used only for the purpose of the administration of criminal justice.

(c) Except as otherwise provided by this Act, conviction record information may be made available for purposes other than the administration of criminal justice only if expressly authorized by applicable State or Federal statute.

(d) Criminal justice information may be made available to qualified persons for research related to the administration of criminal justice under regulations issued by the Federal Information Systems Board, created pursuant to title III. Such regulations shall require preservation of the anonymity of the individuals to whom such information relates, shall require the completion of nondisclosure agreements by all participants in such programs and shall impose such additional requirements and conditions as the Federal Information Systems Board finds to be necessary to assure the protection of privacy and security interests. In formulating regulations pursuant to this section the Board shall develop procedures designed to prevent this section from being used by criminal justice agencies to arbitrarily deny access to criminal justice information to qualified persons for research purposes where they have otherwise expressed a willingness to comply with regulations issued pursuant to this section.

DISSEMINATION OF CERTAIN CRIMINAL JUSTICE INFORMATION TO CRIMINAL JUSTICE AGENCIES

SEC. 202. (a) Except as otherwise provided in this section and in section 203, a criminal justice agency may disseminate to another criminal justice agency only conviction record information.

(b) A criminal justice agency may disseminate arrest record information on an individual to another criminal justice agency—

(1) if that individual has applied for employment at the latter agency and such information is to be used for the sole purpose of screening that application,

(2) if the matter about which the arrest record information pertains has been referred to the latter agency for the purpose of commencing or adjudicating criminal proceedings and that agency may use the information only for a purpose related to that proceeding, or

(3) if the latter agency has arrested, detained, or commenced criminal proceedings against that individual for a subsequent offense, and the arrest record information in the possession of the former agency indicates (A) that there was a prior arrest, detention, or criminal proceeding commenced occurring less than one year prior to the date of the request, and (B) that active prosecution is still pending on the prior charge. In computing the one-year period, time during which the individual was a fugitive shall not be counted. The indication of all revelant facts concerning the status of the prosecution on the prior arrest, detention, or proceeding must be sent to the latter agency and that agency may use the information only for a purpose related to the subsequent arrest, detention, or proceeding.

(c) A criminal justice agency may disseminate criminal history record information on an individual to another criminal justice agency—

(1) if that individual has applied for employment at the latter agency and such information is to be used for the sole purpose of screening that application,

(2) if the matter about which the criminal history record information pertains has been referred to the latter agency for the purpose of commencing or adjudicating criminal proceedings or for the purpose of preparing a pretrial release, posttrial release, or presentence report and that the agency may use the information only for a purpose related to that proceeding or report, or

(3) if the requesting agency has arrested, detained, or commenced criminal proceedings against that individual for a subsequent offense or if the agency is preparing a pretrial release, posttrial release, or presentence report on a subsequent offense and such information is to be used only for a purpose related to that arrest, detention, or proceeding.

(d) A criminal justice agency may disseminate correctional and release information to another criminal justice agency or to the individual to whom the information pertains, or his attorney, where authorized by Federal or State statute.

(e) This section shall not bar any criminal justice agency which lawfully possesses arrest record information from obtaining or disseminating dispositions in order to convert that arrest record information to criminal history information. Nor shall this section bar any criminal justice information system to act as a central repository of such information so long as a State statute expressly so authorizes and so long as that statute would in no way permit that system to violate or to facilitate violation of any provision of this Act. Nor shall this section bar any criminal justice agency from supplying criminal history information to any criminal justice information system established in the Federal Government pursuant to section 307 of this Act.

DISSEMINATION OF IDENTIFICATION RECORD INFORMATION AND WANTED PERSONS RECORD INFORMATION

SEC. 203. Identification record information may be disseminated to criminal justice and to noncriminal justice agencies for any purpose related to the administration of criminal justice. Wanted persons information may be disseminated to criminal justice and noncriminal justice agencies only for the purpose of apprehending the subject of the information.

SECONDARY USE OF CRIMINAL JUSTICE INFORMATION

SEC. 204. Agencies and individuals having access to criminal justice information shall not, directly or through any intermediary, disseminate, orally or in writing, such information to any individual or agency not authorized to have such information nor use such information for a purpose not authorized by this Act: Provided, however, That rehabilitation officials of criminal justice agencies with the consent of the person under their supervision to whom it refers may orally represent the substance of such individual's criminal history record information to prospective employers if such representation is in the judgment of such officials and the individual's attorney, if represented by counsel, helpful to obtaining employment for such individual. In no event shall such correctional officials disseminate records or copies of records of criminal history record information to any unauthorized individual or agency. A court may disclose criminal justice information on an individual in a published opinion or in a public criminal proceeding.

METHOD OF ACCESS AND ACCESS WARRANTS

SEC. 205. (a) Except as provided in subsection 201(d) or in subsection (b) of this section, an automated criminal justice information system may disseminate arrest record information, criminal history record information, or conviction record information on an individual only if the inquiry is based upon positive identification of the individual [illegible] record information. The Federal Information Systems Board shall issue regulations to prevent dissemination of such information except in the above

...974

...inquiries are based upon ... or data elements other ... record information. For ... section "positive identi... identification by means of ... reliable identification ...

...ensuring the provisions of subsec... to arrest record information, criminal history record information, or criminal justice information contained in automated criminal justice information systems on the basis of data elements other than identification record information shall be permissible if the criminal justice agency seeking such access has first obtained a class warrant from a State judge of competent jurisdiction, if the information sought is in the possession of a State or local agency or information system, or from a Federal judge of competent jurisdiction, if the information sought is in the possession of a Federal agency or information system. Such warrants may be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (1) such access is imperative for purposes of the criminal justice agency's responsibilities in the administration of criminal justice and the information sought to be obtained is not reasonably available from any other source or through any other method. A summary of each request for such a warrant, together with a statement of its disposition, shall within ninety days of disposition be furnished the Federal Information Systems Board by the judge.

(c) Access to criminal justice information which has been sealed pursuant to section 206 shall be permissible if the criminal justice agency seeking such access has obtained an access warrant from a State judge of competent jurisdiction of the information sought is in the possession of a State or local agency or information system, or from a Federal judge of competent jurisdiction, if the information sought is in the possession of a Federal agency or information system. Such warrants may be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (1) such access is imperative for purposes of the criminal justice agency's responsibilities in the administration of criminal justice, and (2) the information sought to be obtained is not reasonably available from any other source or through any other method.

SECURITY, ACCURACY, UPDATING, AND PURGING

SEC. 206. Each criminal justice information system shall adopt procedures reasonably designed—

(a) To insure the physical security of the system, to prevent the unauthorized disclosure of the information contained in the system, and to insure that the criminal justice information in the system is currently and accurately revised to include subsequently received information. The procedures shall also insure that all agencies to which such records are disseminated or from which they are collected are currently and accurately informed of any correction, deletion, or revision of the records. Such regulations shall require that automated systems shall as soon as technically feasible inform any other information system or agency which has direct access to criminal justice information contained in the automated system of any disposition relating to arrest record information on an individual or any other change in criminal justice information in the automated system's possession.

(b) To insure that criminal justice information is purged or sealed when required by State or Federal statute, State or Federal regulations, or court order, or when, based on considerations of age, nature of the record or the interval following the last entry of information indicating that the individual is under the jurisdiction of a criminal justice agency, the information is unlikely to provide a reliable guide to the behavior of the individual. Such procedures shall, as a minimum, provide—

(1) for the prompt sealing or purging of criminal justice information relating to an individual who has been free from the jurisdiction or supervision of any law enforcement agency for (A) a period of seven years if such individual has previously been convicted of an offense classified as a felony under the laws of the jurisdiction which such conviction occurred, or (B) a period of five years, if such individual has previously been convicted of a nonfelonious offense as classified under the laws of the jurisdiction where such conviction occurred, or (C) a period of five years if no conviction of the individual occurred during that period, no prosecution is pending at the end of the period, and the individual is not a fugitive; and

(2) for the prompt sealing or purging of criminal history record information in any case in which the police have elected not to refer the case to the prosecutor or in which the prosecutor has elected not to commence criminal proceedings.

(c) To insure that criminal justice agency personnel may use or disseminate criminal justice information only after determining it to be the most accurate and complete information available to the criminal justice agency. Such regulations shall require that, if technically feasible, prior to the dissemination of arrest record information by automated criminal justice information systems, an inquiry is automatically made of and a response received from the agency which contributed that information to the system to determine whether a disposition is available.

(d) To insure that information may not be submitted, modified, updated, disseminated, or removed from any criminal justice information system without verification of the identity of the individual to whom the information refers and an indication of the person or agency submitting, modifying, updating, or removing the information.

ACCESS BY INDIVIDUALS FOR PURPOSES OF CHALLENGE

SEC. 207. (a) Any individual who believes that a criminal justice information system or criminal justice agency maintains criminal justice information concerning him, shall upon satisfactory verification of his identity, be entitled to review such information in person or through counsel and to obtain a certified copy of it for the purpose of challenge, correction, or the addition of explanatory material, and in accordance with rules adopted pursuant to this section, to challenge, purge, seal, delete, correct, and append explanatory material.

(b) Each criminal justice agency and criminal justice information system shall adopt and publish regulations to implement this section which shall, as a minimum, provide—

(1) the time, place, fees to the extent authorized by statute, and procedure to be followed by an individual or his attorney in gaining access to criminal justice information;

(2) that any individual whose record is not purged, sealed, modified, or supplemented after he has so requested in writing shall be entitled to a hearing within thirty days of such request before an official of the agency or information system authorized to purge, seal, modify, or supplement the criminal justice information at which time the individual may appear with counsel, present evidence, and examine and cross-examine witnesses;

(3) any record found after such a hearing to be inaccurate, incomplete, or improperly maintained shall, within thirty days of the date of such finding, be appropriately modified, supplemented, purged, or sealed;

(4) each criminal justice information system shall keep and, upon request, disclose to each person the name of all persons or organizations, criminal justice agencies, noncriminal justice agencies, or criminal justice information systems to which the date upon which such criminal justice information was disseminated;

(5) (A) beginning on the date that a challenge has been made to criminal justice information pursuant to this section, and until such time as that challenge is finally resolved, any criminal justice agency or information system which possesses the information shall disseminate the fact of such challenge each time it disseminates the challenged criminal justice information. In the case of a challenge to criminal justice information maintained by an automated criminal justice information system, such system shall automatically inform any other information system or criminal justice agency to which such automated system has disseminated the challenged information in the past, of the fact of the challenge and its status;

(B) if any corrective action is taken as a result of a review or challenge filed pursuant to this section, any agency or system which maintains or has ever received the uncorrected criminal justice information shall be notified as soon as practicable of such correction and immediately correct its records of such information. In the case of the correction of criminal justice information maintained by an automated criminal justice information system, any agency or system which maintains or has ever received the uncorrected criminal justice information shall if technically feasible be notified immediately of such correction and shall immediately correct its records of such information; and

(6) the action or inaction of a criminal justice information system or criminal justice agency on a request to review and challenge criminal justice information in its possession as provided by this section shall be reviewable by the appropriate United States district court pursuant to a civil action under section 308.

(c) No individual who, in accord with this section, obtains criminal justice information regarding himself may be required or requested to show or transfer records of that information to any other person or any other public or private agency or organization: *Provided, however,* That if a Federal or State statute expressly so authorizes, conviction record information may be disseminated to noncriminal justice agencies and an individual might be requested or required to show or transfer copies of records of such conviction record information to such noncriminal justice agencies.

INTELLIGENCE SYSTEMS

SEC. 208. (a) Criminal justice intelligence information shall not be maintained in criminal justice information systems.

(b) Criminal justice intelligence information shall not be maintained in automated systems.

TITLE III—ADMINISTRATIVE PROVISIONS; REGULATIONS; CIVIL REMEDIES; CRIMINAL PENALTIES

FEDERAL INFORMATION SYSTEMS BOARD

SEC. 301. (a) CREATION AND MEMBERSHIP.—There is hereby created a Federal Information Systems Board (hereinafter the "Board") which shall have overall responsibility for the administration and enforcement of this Act. The Board shall be composed of nine members. One of the members shall be the Attorney General and two of the members shall be designated by the President as representatives of other agencies outside of the Department of Justice. The six remaining members shall be appointed by the President with the advice and consent of the Senate. Of the six members appointed by the President, three shall be either directors of statewide criminal justice information systems or members of the Federal Information Systems Advisory Committee at the time of their appointment. The three remaining Presidential appointees shall be private citizens well

versed in the law of privacy, constitutional law, and information systems technology. The President shall designate one of the six Presidential appointees as Chairman and such designation shall also be confirmed by the advice and consent of the Senate.

(b) COMPENSATION OF MEMBERS AND QUORUM.—Members of the Board appointed by the President shall be compensated at the rate of $100 per day for each day spent in the work of the Board, and shall be paid actual travel expenses and per diem in lieu of subsistence expenses when away from their usual places of residence, as authorized by section 5703 of title 5, United States Code. Five members shall constitute a quorum for the transaction of business.

(c) AUTHORITY.—For the purpose of carrying out its responsibilities under the Act the Board shall have authority to—

(1) issue regulations as required by section 303;

(2) review and disapprove of regulations issued by a State agency pursuant to section 304 or by any criminal justice agency which the Board finds to be inconsistent with this Act;

(3) exercise the powers set out in subsection 307(d);

(4) bring actions under section 308 for declaratory and injunctive relief;

(5) operate an information system for the exchange of criminal justice information among the States and with the Federal Government pursuant to section 307;

(6) supervise the installation and operation of any criminal justice information system or criminal justice intelligence information system operated by the Federal Government;

(7) conduct an ongoing study of the policies of various agencies of the Federal Government in the operation of information systems;

(8) require any department or agency of the Federal Government or any criminal justice agency to submit to the Board such information and reports with respect to its policy and operation of information systems or with respect to its collection and dissemination of criminal justice information or criminal justice intelligence information and such department or agency shall submit to the Board such information and reports as the Board may reasonably require; and

(9) conduct audits as required by section 306.

(d) OFFICERS AND EMPLOYEES.—The Board may appoint and fix the compensation of a staff director, legal counsel, and such other staff personnel as it deems appropriate.

(e) REPORT TO CONGRESS AND TO THE PRESIDENT.—The Board shall issue an annual report to the Congress and to the President. Such report shall at a minimum contain—

(1) the results of audits conducted pursuant to section 306;

(2) a summary of public notices filed by criminal justice information systems, criminal justice intelligence information systems, and criminal justice agencies pursuant to section 305; and

(3) any recommendations the Board might have for new legislation on the operation or control of information systems or on the collection and control of criminal justice information or criminal justice intelligence information.

FEDERAL INFORMATION SYSTEMS ADVISORY COMMITTEE

SEC. 302. (a) CREATION AND MEMBERSHIP.—There is hereby created a Federal Information Systems Advisory Committee (hereinafter called the Committee) which shall advise the Board on its activities. The Committee shall be composed of one representative from each State appointed by the Governor, who shall serve at the pleasure of the Governor. However, once the State has created an agency pursuant to subsection 304 (b), the State's representative on the Committee shall be designated by that agency and shall serve at the pleasure of that agency.

(b) CHAIRMAN AND SUBCOMMITTEE.—The Committee shall be convened by the Board and at its first meeting shall elect a chairman from its membership. The Committee may create an executive committee and such other subcommittees as it deems necessary.

(c) AUTHORITY.—The Committee shall make any recommendations it deems appropriate to the Board concerning the Board's responsibilities under this Act, including its recommendations concerning regulations to be issued by the Board pursuant to section 303, concerning the Board's operation of interstate information systems pursuant to section 307, and concerning any recommendations which the Board might make in its annual report to Congress and the President.

(d) OFFICERS AND EMPLOYEES.—The Committee shall have access to the services and facilities of the Board and if the Board deems necessary the Committee shall have its own staff.

FEDERAL REGULATIONS

SEC. 303. The Board shall, after appropriate consultation with the Committee and other representatives of State and local criminal justice agencies participating in information systems covered by this Act and other interested parties, promulgate such rules, regulations, and procedures as it may deem necessary to effectuate the provisions of this Act. The Board shall follow the provisions of the Administrative Procedures Act with respect to the issuance of such rules. All regulations issued by the Board or any criminal justice agency pursuant to this Act shall be published and easily accessible to the public.

STATE REGULATIONS AND CREATION OF STATE INFORMATION SYSTEMS BOARD

SEC. 304. Beginning two years after enactment of this Act, no criminal justice agency shall collect criminal justice information from, nor disseminate criminal justice information to, a criminal justice agency—

(a) which has not adopted all of the operating procedures required by sections 206 and 207 and necessitated by other provisions of the Act; or

(b) which is located in a State which has failed to create a State information systems board. The State information systems board shall be an administrative body which is separate and apart from existing criminal justice agencies and which will have statewide authority and responsibility for:

(1) the enforcement of the provisions of this Act and any State statute which serves the same goals;

(2) the issuance of regulations, not inconsistent with this Act, regulating the exchange of criminal justice information and criminal justice intelligence information systems and the operation of criminal justice information systems and the operation of criminal justice intelligence information systems; and

(3) the supervision of the installation of criminal justice information systems, and criminal justice intelligence information systems, the exchange of information by such systems within that State and with similar systems and criminal justice agencies in other States and in the Federal Government.

PUBLIC NOTICE REQUIREMENT

SEC. 305. (a) Any criminal justice agency maintaining an automated criminal justice information system or a criminal justice intelligence information system shall give public notice of the existence and character of its system once each year. Any agency maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any agency proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall be transmitted to the Board and shall specify—

(1) the name of the system;

(2) the nature and purposes of the system;

(3) the categories and number of persons on whom data are maintained;

(4) the categories of data maintained, indicating which categories are stored in computer-accessible files;

(5) the agency's operating rules and regulations issued pursuant to section 206 and 207, the agency's policies and practices regarding data information storage, duration of retention of information, and disposal thereof;

(6) the categories of information sources;

(7) a description of all types of use made of information, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them; and

(8) the title, name, and address of the person immediately responsible for the system.

(b) Any criminal justice agency, criminal justice information system, or criminal justice intelligence information sysem operated by the Federal Government shall satisfy the public notice requirement set out in subsection (a) of this section by publishing the information required by that subsection in the Federal Register.

ANNUAL AUDIT

SEC. 306. (a) At least once annually the Board shall conduct a random audit of the practices and procedures of the Federal agencies which collect and disseminate information pursuant to this Act to insure compliance with its requirements and restrictions. The Board shall also conduct such an audit of at least ten statewide criminal justice information systems each year and of every statewide and multistate system at least once every five years.

(b) Each criminal justice information system shall conduct a similar audit of its own practices and procedures once annually. Each State agency created pursuant to subsection 304(b) shall conduct an audit on each criminal justice information system and each criminal justice intelligence information system operating in that State on a random basis, at least once every five years.

(c) The results of such audits shall be made available to the Board which shall report the results of such audits once annually to the Congress by May 1 of each year beginning on May 1 following the first full calendar year after the effective date of the Act.

PARTICIPATION BY THE BOARD

SEC. 307. (a) Subject to the limtations of subsections (b) and (c) of this section, the Board may participate in interstate criminal justice information systems, including the provision of central information storage facilities and telecommunications lines for interstate transmission of information.

(b) Facilities operated by the Board may include criminal history record information on an individual relating to a violation of the criminal laws of the United States, violations of the criminal laws of two or more States, or a violation of the laws of another nation. As to all other individuals, criminal justice information included in Board facilities shall consist only of information sufficient to establish the identity of the individuals, and the identities and locations of criminal justice agencies possessing other types of criminal justice information concerning such individuals.

(c) Notwithstanding the provisions of subsection (b), the Board may maintain

criminal history record information submitted by a State which otherwise would be unable to participate fully in a criminal history record information system because of the lack of facilities or procedures but only until such time as such State is able to provide the facilities and procedures to maintain the records in the State, and in no case for more than five years. Criminal history record information maintained in Federal facilities pursuant to this subsection shall be limited to information on offenses classified as felonies under the jurisdiction where such offense occurred.

(d) If the Board finds that any criminal justice information system or criminal justice agency has violated any provision of this Act, it may (1) interrupt or terminate the exchange of information as authorized by this section, or (2) interrupt or terminate the use of Federal funds for the operation of such a system or agency, or (3) require the system or agency to return Federal funds distributed in the past, or it may take any combination of such actions or (4) require the system or agency to discipline any employee responsible for such violation.

CIVIL REMEDIES

SEC. 308. (a) Any person aggrieved by a violation of this Act shall have a civil action for damages or any other appropriate remedy against any person, system, or agency responsible for such violation after he has exhausted the administrative remedies provided by section 207.

(b) The Board or any State agency created pursuant to subsection 304(b) shall have a civil action for declaratory judgments, cease and desist orders, and such other injunctive relief against any criminal justice agency, criminal justice information system, or criminal justice intelligence information system within its regulatory jurisdiction.

(c) Such person, agency, or the Board may bring a civil action under this Act in any district court of the United States for the district in which the violation occurs, or in any district court of the United States in which such person resides or conducts business, or has his principal place of business, or in the District Court of the United States for the District of Columbia.

(d) The United States district court in which an action is brought under this Act shall have exclusive jurisdiction without regard to the amount in controversy. In any action brought pursuant to this Act, the court may in its discretion issue an order enjoining maintenance or dissemination of information in violation of this Act, or correcting records of such information or any other appropriate remedy except that in an action brought pursuant to subsection (b) the court may order only declaratory or injuctive relief. In any action brought pursuant to this Act the court may also order the Board to conduct an audit of the practices and procedures of the agency in question to determine whether information is being collected and disseminated in a manner inconsistent with the provisions of this Act.

(e) In an action brought pursuant to subsection (a), any person aggrieved by a violation of this Act shall be entitled to a $100 recovery for each violation plus actual and general damages and reasonable attorneys' fees and other litigation costs reasonably incurred. Exemplary and punitive damages may be granted by the court in appropriate cases brought pursuant to subsection (a). Any person, system, or agency responsible for violations of this Act shall be jointly and severally liable to the person aggrieved for damages granted pursuant to this subsection. Any criminal justice information system or any criminal justice intelligence information system which facilitates the transfer of information in violation of this Act shall be jointly and severally liable along with any criminal justice agency or person responsible for a violation of this Act.

(g) For the purposes of this Act the United States shall be deemed to have consented to suit and any agency or system operated by the United States, found responsible for a violation shall be liable for damages, reasonable attorneys' fees, and litigation cost as provided in subsection (f) notwithstanding any provisions of the Federal Tort Claims Act.

CRIMINAL PENALTIES

SEC. 309. Whoever willfully disseminates, maintains, or uses information knowing such dissemination, maintenance, or use to be in violation of this Act shall be fined not more than $5,000 or imprisoned for not more than five years, or both.

PRECEDENCE OF STATE LAWS

SEC. 310. (a) Any State law or regulation which places greater restrictions upon the dissemination of criminal justice information or criminal justice intelligence information or the operation of criminal justice information systems or criminal justice intelligence information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in this Act shall take precedence over this Act or regulations issued pursuant to this Act.

(b) Any State law or regulation which places greater restrictions upon the dissemination of criminal justice information or criminal justice intelligence information or the operation of criminal justice information systems or criminal justice intelligence information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in the State law or regulations of another State shall take precedence over the law or regulations of the latter State where such information is disseminated from an agency or information system in the former State to an agency, information system, or individual in the latter State. Subject to court review pursuant to section 308, the Board shall be the final authority to determine whether a State statute or regulation shall take precedence under this section and shall as a general matter have final authority to determine whether any regulations issued by a State agency, a criminal justice agency, or information system violate this Act and are therefore null and void.

APPROPRIATIONS AUTHORIZED

SEC. 311. For the purpose of carrying out the provisions of this Act there are authorized to be appropriated such sums as the Congress deems necessary.

SEVERABILITY

SEC. 312. If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

REPEALERS

SEC. 313. The second paragraph under the headings entitled "Federal Bureau of Investigation; Salaries and Expenses" contained in the "Department of Justice Appropriations Act, 1973" is hereby repealed.

EFFECTIVE DATE

SEC. 314. The provisions of this Act shall take effect upon the date of expiration of the one-hundred-and-eighty-day period following the date of the enactment of this Act: *Provided, however,* That section 311 of this Act shall take effect upon the date of enactment of this Act.

CRIMINAL JUSTICE INFORMATION CONTROL AND PROTECTION OF PRIVACY ACT OF 1974

SECTION-BY-SECTION DISCUSSION

Title I—Findings and declaration of policy: definitions

Section 101 summarizes the constitutional, legal and practical reasons Congress is taking action to regulate the exchange of criminal justice information. It also states the constitutional authority to legislate: the Commerce clause and the Federal participation in state and interstate information systems.

Section 102 lists definitions of terms used in the proposed legislation. The definitions are important because they establish the scope of coverage of the legislation. For example "criminal justice agency" is defined so that the restrictions on data collection and dissemination contained in the bill cover any state, local or Federal governmental agency maintaining such data.

"Criminal justice information" is defined so that limited exchange of routine information reflecting the status of a criminal case and its history, or reports compiled for bail or probation can be exchanged between governmental agencies. All other information referenced under an individual's name and related to criminal activity is called "criminal justice intelligence" and is placed under stricter limitations.

Title II—Collection and dissemination of criminal justice information and criminal justice intelligence information

Section 201 sets the general policy on the collection and dissemination of criminal justice information. Criminal justice information can only be used for criminal justice purposes unless a state or Federal statute specifically authorizes dissemination of conviction records to non-criminal justice agencies. The section permits researchers access to the information only if the privacy of the subjects of the information is protected.

Sections 202 and 203 deal with the exchange of criminal justice information among criminal justice agencies. The general rule is that only conviction records may be exchanged. However, there are limited exceptions to that general rule. For example, corrections and release information can be disseminated outside of the agency which collected it only where expressly authorized by state or Federal statute. Fingerprint information may be freely disseminated as long as no stigma is attached. Wanted persons information, that is identifying information on a fugitive, may be disseminated liberally for the purpose of apprehending the fugitive. Raw arrest records and records of criminal proceedings which did not result in conviction could be exchanged in certain carefully defined situations.

Section 204 prohibits agencies or persons who lawfully gain access to information from using the information for a purpose or from disseminating the information in a manner not permitted by the legislation.

Section 205 is based on a provision contained in Project SEARCH's model state statute and the Massachusetts arrest records statute. It places limitations on access to criminal justice information via categories other than name. For example, it would require investigators to get a court order before accessing a criminal justice data bank by offense—i.e., a printout on all persons charged with Burglary I with certain physical descriptions and from a certain geographical area. According to the commentary on the SEARCH model statute: "(the provision) is modeled on the provisions which now govern wiretapping and electronic eavesdropping. It is intended to interpose the judgment of an impartial magistrate to control the usage of an investigative method that may, if misused, create important hazards for individual

privacy". Section 205 creates a similar procedure for the opening of sealed records.

Section 206 requires every agency or information system covered by the act to promulgate regulations on security, accuracy, updating and purging and sets out in general terms what those regulations must provide. The regulations must provide a method for informing users of changes in disseminated information and for the purging of old, outdated and irrelevant information.

Section 207 requires every agency or information system covered by the act to establish a process for access and challenge of incorrect or inaccurate information. The section sets out in considerable detail what those regulations must provide. This section should be read along with section 308 which provides court review procedures where the agency fails to comply with section 207 or any other provision of the Act.

Section 208 places simple but very strict limitations on the collection and dissemination of intelligence information. Such information may not be maintained in automated systems and must be kept separate and apart from all other criminal justice files.

Title III—Administrative provisions; regulations; civil remedies; criminal penalties

Title III creates a novel Federal-state administrative structure for enforcement of the Act. Section 301 establishes a Federal Information Systems Board, an independent agency with general responsibility for administration and enforcement of the Act. The Board would be composed of representatives of the Department of Justice and two other Federal agencies, plus six other members nominated by the President, with the advice and consent of the Senate. Of the latter six members, three must be representatives of state governments and three private citizens well versed in civil liberties and computer technology. The President would also designate a chairman from the latter six members.

The Board would have the authority to issue general regulations applying the Act's policies. It could operate the interstate information system authorized by section 307. It would conduct audits pursuant to section 306, and would have other necessary enumerated powers as well as authority to conduct general studies of information systems and make recommendations to the Congress for additional legislation.

Section 302 creates an Information Systems Advisory Committee composed of one representative from each state. The Committee shall advise the Board on all of the Board's responsibilities under the Act and in particular provide advice on the Board's operation of the interstate information system established pursuant to Section 307 and the Board's promulgation of regulations pursuant to Section 303.

Section 303 requires the Federal Information Systems Board to issue regulations with implement this Act.

Section 304 requires each state to establish a central administrative agency, separate and apart from existing criminal justice agencies, with broad authority to oversee and regulate the operation of criminal justice information systems in that state. This section is based upon the concept embodied in the Project SEARCH model statute and the Massachusetts statute. Beginning two years after enactment no information system or agency could exchange information with a system or agency in a state which has not created such an agency or with a system or agency which has not adopted all of the regulations required by sections 206 and 207 or elsewhere in the Act.

Section 305 is based upon a suggestion contained in the Report of the Secretary's Advisory Committee on Automated Personal Data Systems of the Department of Health, Education, and Welfare. It requires every information system or agency [illegible] notice, once annually, of the type of information it collects and disseminates, its sources, purpose, function, administrative director or other pertinent information. It also requires every system or agency to give public notice of an expansion and any new system to give public notice before it becomes operational so that interested parties will have an opportunity to comment.

Section 306 requires audits of systems and agencies which collect and disseminate information. The audits are to be conducted by the Federal Information Systems Board, by an independent state agency created pursuant to Section 304 and by each criminal justice agency.

Section 307 is a general grant of authority permitting the Federal Government to operate an interstate criminal justice information system under the policy control of the Feedral-State board. However, the Federal role is carefully circumscribed. Information contained in such a Federal system is limited to a simple index containing the subject's name and the name of the state or local agency which possesses a more complete file. The Federal Information Systems Board could maintain more complete files on violations of a criminal law of the United States, violations of the criminal law of two or more states, or violations of the laws of another nation. Only persons charged with felonies could be listed in the data banks. If a given state lacks the facilities to operate an automated information system the Information Systems Board could provide the facilities for a period of five years.

The section also lists certain administrative actions that may be taken by the Federal Information Systems Board in the event that a criminal justice information system is found to have violated any provision of the Act.

Section 308 provides the judicial machinery for the exercise of the right granted in Section 207 and elsewhere in the Act. The aggrieved individual may obtain both injunctive relief and damages, $100 recovery for each violation, actual and general damages, attorney's fees, and other litigation costs whether violations were willful or negligent.

Section 309 provides criminal penalties for violations of the Act.

Section 310 provides that any state statute, state regulation or Federal regulation which imposes stricter privacy requirements on the operation of criminal justice information systems or upon the exchange of criminal justice information takes precedence over this Act or any regulations issued pursuant to this Act or any other state law when a conflict arises. Subject to court review pursuant to section 308, the Federal Information Systems Board would make the administrative decision as to which statute or regulation governs, and whether a regulation comports with this Act.

Section 311 authorizes the appropriation of such funds as the Congress deems necessary for the purposes of the Act.

Section 312 is a standard severability provision.

Section 313 repeals a temporary authority for the Federal Bureau of Investigation to disseminate Rap sheets to non-criminal justice agencies.

Section 314 makes this Act effective six months after its enactment.

[From the New York Times, Jan. 10, 1974]

THREE BROTHERS

(By William Safire)

WASHINGTON, January 9.—"Little Brother" is watching you.

The poking and prying into an individual's private life by "Big Brother"—the Federal Government—is a matter of great concern, but the less-publicized snooping of "little" and "middle" brothers is more pervasive and [illegible]

"Little Brother" is the hard-to-reach private organization that determines whether or not you are a good retail credit risk. Deadbeats do not deserve credit, but a great many honest livebeats have found themselves denied the right to live life on the installment plan because of computer foul-ups or the indelibly recorded judgments of vindictive neighbors.

The Fair Credit Reporting Act of 1970 helps the determined credit rejectee to find out who is rattling his rating, but "Little Brother" is still hard to find and nearly impossible to budge.

Right now, at State of the Union time, President Nixon is considering a proposal that would come to the aid of the individual's battered right to privacy in these ways:

1. Making it possible for an individual to see what is in his credit record and how it is being used;

2. Enabling that credit-seeker to correct and amend information that is inaccurate or incomplete;

3. Placing a legal "burden of reliability" on credit agencies so that they must take precautions against abuse of their files;

4. Preventing the use of information that people give about themselves for one purpose from being used for another purpose—which happens when you send in your address to receive an item and wind up on some mailing lists you don't want to be on.

5. Requiring agencies that ask individuals for information to inform them whether they are legally required to provide it. Sometimes you have to answer the Census Bureau, for example, and sometimes you can tell their doorbell-ringers to get lost.

Such proposals to shore up privacy are creditable, so to speak; so is an idea now being discussed in the White House to put restraints on "Middle Brother," the computerized cooperation between local police departments and state and Federal law enforcement agencies.

Police officials should have a quick way of identifying suspects or examining far-off records of previous convictions, and the F.B.I.'s National Crime Information Center has long been available to state agencies—but once placed in computers, how secure will F.B.I. files be? When does sensible record-keeping become a dreaded "dossierization"?

One of the hottest controversies raging within the law-enforcement community is whether computers used by lawmen should be "dedicated" or "shared." Computer salesmen say it is cheaper and more efficient to "share" giant computers with banks and insurance companies, rather than to dedicate a computer to police work alone—but there is the danger of a smart programmer breaking the police code and having access to information that should be confidential.

Sounds esoteric—but a mistake here could put a crimp in privacy for decades to come. The legislative proposal the President is mulling over would make the Federal Law Enforcement Assistance Administration, which would put up the money for computerization, aware of the need for the most stringent safeguards.

This White House interest in curbing both little and middle brother is vital and welcome but it does not deal with the privacy question now on the front burner: warrantless wiretaps, the encroachment on Fourth Amendment protections by "Big Brother."

Such tapping was declared illegal by the Supreme Court in 1971; since then, no taps can be placed directly on American citizens even in national security cases without a court warrant—at least, that's how a nervous White House interprets the Supreme Court decision.

President Nixon is not one to cheerfully give away any of the powers of office, but the man who opened Pandora's Box of cavesdropping would be well advised to help nail down the lid.

[illegible] would be to do away with

warrantless wiretaps entirely, forcing future Attorneys General to go to Federal judges for permission to do any tapping. This would drive the intelligence community up the wall; but isn't warrantless wiretapping a danger to liberty that outweighs the advantage of listening in to foreign embassies—especially when they know we're listening?

Since the state of this Union has been so deeply afflicted by matters related to eavesdropping, the President does well to think about civil liberties in dealing with the "little brother" of credit ratings and the "middle brother" of computerized police records. But that still leaves Big Brother. If the President were to take the lead in doing away with warrantless wiretaps, he would astound his friends, confound his critics and show history he was able to profit from his most costly lesson.

[From the New York Times, Feb. 5, 1974]

MR. NIXON DISCOVERS PRIVACY

(By Tom Wicker)

Skeptical chuckles may have seemed in order when Richard Nixon promised in his 1974 State of the Union Message a "major initiative" and a "cabinet-level review" on the matter of privacy—particularly on safeguarding information stored in computers by interlinked Federal and state criminal justice agencies. Mr. Nixon, after all, had wiretapped his own staff and his Administration had failed since 1970 to take such a "major initiative," despite the repeated requests of Congress that it do so.

But never mind the chuckles. The Justice Department immediately followed the State of the Union Message with the detailed legislative proposal so long awaited. Beyond that, Senator Sam J. Ervin Jr., chairman of the constitutional rights subcommittee, is ready with his own more restrictive bill, and the prospects seem brighter than they ever have been for action at last.

"At last" is not too strong a phrase. Sweden, for example, passed in April 1973, a comprehensive law governing the collection and dissemination of criminal justice information. But little has been done here, although in recent years Federal funding through the Law Enforcement Assistance Administration has achieved a phenomenal growth of criminal justice data banks throughout most of the states; all fifty soon will be involved in the system.

Interlinked among themselves and with the massive Federal system operated by the F.B.I., these data banks are collecting an enormous amount of information about millions of American citizens, by no means all of them criminal offenders. The nature, use and distribution of that information is virtually unregulated by anyone; as noted here before, Massachusetts alone found last year that more than 75 public and private agencies having nothing to do with criminal justice had achieved regular access to its criminal offender files.

The Department of Justice bill would go far to fill this void, by providing as a matter of law that individuals could review their own records, correct inaccuracies and sue anyone disclosing the information improperly. The measure also would sharply limit those to whom any of the records could be disclosed, and require the sealing of individual records after a specified time.

Senator Ervin's proposal would improve on the Justice Department bill in important respects. For example, it would provide that an arrest record showing no subsequent disposition of the case, or one showing an acquittal or that the case had been dropped, would be "programmed" out of the reach of criminal justice agencies as well as any other public or private inquirers one year after the original arrest. Even during that first year, such a record would be available to police only if the person involved was re-arrested on some other charge.

More importantly, the Ervin bill would place the entire Federal, state and interstate criminal justice data system under the regulation of a nine-man board—one representative each from the Department of Justice and two other interested Federal agencies three representatives from involved state agencies, and three representatives of the public at large, all appointed by the President and confirmed by the Senate.

This board would remove the system from the exclusive control of police and criminal justice agencies, provide some amelioration of Federal domination, and—so Mr. Ervin hopes—establish an effective instrument for efficient and equitable regulation of unforeseen problems as they arise, with the necessity for new legislation.

All this is strong medicine for some criminal justice organizations to swallow; predictably enough, Clarence M. Kelley, the director of the F.B.I., has declined full endorsement of even the Justice Department bill. He is reported to be reflecting the views of numerous police departments, particularly on the matter of sealing—that is, closing to any inquirer—criminal records seven years following the subject's release from custody on a felony conviction (five years in misdemeanor cases). Some other Federal agencies with an interest in criminal justice records also have reservations about the Justice Department bill, raising the question whether it really is an "Administration proposal."

Nevertheless, Mr. Nixon himself is on the record at least pro forma; Mr. Ervin plans to be a cosponsor of the Justice Department measure, and such Nixon stalwarts as Roman Hruska of Nebraska and Milton Young of North Dakota have been induced to cosponsor the Ervin bill. This cross-sponsorship bodes well for some kind of regulatory legislation, and almost any would be an improvement on the present vacuum.

At the least, the need for control has been stated at the highest level; both the Justice and Ervin bills recognize the principle that those who compile and operate the data banks should not have discretion to determine their use; and even while declining endorsement of a specific bill, Director Kelley said he welcomed legislation to "insure the maximum protection of individual rights."

[From the Washington Post, Feb. 4, 1974]

CONTROLLING THE DATA BANKS

President Nixon was absolutely right in his State of the Union address when he included protection of individual privacy among those issues which should get legislative attention this year. Since Mr. Nixon is a very recent convert to this view, many uncertainties remain about how quickly and fully the commitment will be translated into specific policies. Thus it is doubly encouraging that the Department of Justice is proceeding at once to send Congress its long-waited bill to control federal, state and interstate criminal justice data banks.

The unveiling of any comprehensive administration measure on criminal records would be reason for some celebration. The Congress first requested recommendations from the Justice Department back in 1970, but the response was half-hearted at best until former Attorney General Elliot Richardson made the subject a personal priority last year. Attorney General William Saxbe has followed through, and the result is a rather impressive bill which sets out broad, general policies intended to insure that all criminal records in automated or interstate files will be accurate, timely and complete, that individuals will be able to review and correct files on themselves, and that there will be far less trafficking in criminal records among public and private agencies outside the law enforcement field.

Some points of contention remain. Within the administration, the FBI is said to be less than enthusiastic about the new bill, and several other federal agencies will probably be going to Congress on their own to seek authorization to continue current practices such as checking the criminal records of job and credit applicants. On Capitol Hill, Sen. Sam J. Ervin (D–N.C.) is ready to introduce his own regulatory bill. The Ervin proposal is more stringent and detailed than the Justice Department measure in several important respects, and it would also transfer regulatory authority over federal criminal history files from the Justice Department to an independent federal-state board. But it appears that this year such substantive issues can finally be seriously addressed—and even resolved with some harmony and dispatch—because a good working alliance is developing among Senator Ervin, the Justice Department and Sen. Roman Hruska (R-Neb.), ranking Republican on the Senate Judiciary Committee and a potential pivotal figure in the discussion to come.

Thus on the top-priority privacy issue of criminal records, the debate has advanced from whether Congress should legislate anything to what kind of bill should be passed. The outlook is not so promising, however, on related fronts. While endorsing the protection of privacy as a general principle the other night, Mr Nixon did not propose any specifics. Instead, he simply announced another study—"an extensive Cabinet-level review" of government and industry practices impinging on privacy. Thus the President seems to have shelved, among other things, the report of the HEW advisory panel which called for a code of "fair information practices" for all federal data banks. He also seems to have postponed any positive administration involvement in the congressional efforts to deal with such specific problems as credit reporting, the secrecy of bank records and the rights of participants in federal programs.

The most striking flaw in Mr. Nixon's approach was his definition of the "privacy problem" primarily as a function of advancing technology. Computers have indeed eroded man's ability to control who knows how much about a person's private life and how such knowledge is used. But the basic problem is less the capability of machines than the curiosity of man, particularly the curiosity of those in positions of power over the lives of their fellow citizens. We need no further studies of the potential dangers of official nosiness—wiretapping, bugging, illegal searches, political surveillance, harassment of dissident groups, and the other abuses and excesses which have aroused such public concern. Mr. Nixon did not address himself to this subject at all. Until he does so, his commitment to protecting privacy will remain vague and incomplete.

Mr. HRUSKA. Mr. President, I should like to congratulate and commend the distinguished Senator from North Carolina (Mr. ERVIN) for the very well prepared, well organized, documented, and competently assembled statement he has just presented concerning criminal justice information systems.

It is a splendid opening statement on a very vital subject. I believe that its tenor testifies well to the vast scope and the complexity of the area of law with which it is concerned.

It will be considered a classic, I am sure, and will be often cited because of its fine discussion of the law and the techniques regarding criminal data systems, as well as the general philosophy

which the Senator from North Carolina spells out in his excellent manner.

Much work and many studies have been devoted to this subject.

The Senator from North Carolina has alluded to many of those facets, and all of us can be impressed by the far-reaching consequences of the failure to act, with deliberation, to be sure, and yet, as expeditiously as wisely and practicable to deal with the bills introduced today.

Again I commend the Senator from North Carolina and congratulate him for his very fine contribution.

INTRODUCTION OF S. 2964—CRIMINAL SYSTEMS ACT OF 1974

Mr. HRUSKA. Mr. President, I am pleased to introduce on behalf of the Department of Justice a bill entitled "Criminal Justice Information Systems Act of 1974," S. 2964. I send it to the desk and ask that it be appropriately referred.

The PRESIDING OFFICER (Mr. HELMS). The bill will be received and appropriately referred.

Mr. HRUSKA. Mr. President, this bill will provide for and facilitate the collection, classification, maintenance, and use of criminal justice information; and also make provision for and regulate access thereto, as well as uses and dissemination thereof. It is intended to provide strong safeguards against unwarranted violation of privacy of the individuals to whom such information pertains, and to insure physical security and integrity of criminal justice information systems, and for other related purposes.

At the same time, I am further pleased to cosponsor with my valued friend, the distinguished senior Senator from North Carolina (Mr. ERVIN), the Criminal Justice Information Control and Protection of Privacy Act of 1974, S. 2963, which he introduced earlier this afternoon, and of which he is the author. Senator ERVIN's bill takes a somewhat different approach to several aspects of the subject than are contained in the bill which I have introduced, but generally their respective fundamental objectives, thrust, and other provisions parallel each other.

Mr. President, in introducing the one bill and in cosponsoring the other, it should be made clear that I am not indorsing or approving either in its entirety. The thrust, the fundamental objectives, and in many provisions, yes, there is indorsement and approval. Some of the cosponsors to the bill I am introducing have also expressed this thought. But in each there are a number of provisions which must be subjected to close scrutiny, searching analysis, and full study before they are accepted, modified, or rejected. Certain of the provisions in each bill will be controversial and even mutually exclusive so that a choice will be mandatory. Indeed there is much room for debate and sincere difference of opinion.

As to some of such instances as they are now drafted I find that I myself have not reached a firm judgment.

But, Mr. President, both of these bills have much merit. Both will be excellent vehicles to serve as bases for hearings and legislation on the pertinent subject matter. It is with this thought in mind that I have expressed favor for each, namely, that we will hear from various witnesses the opposing views and elicit more complete information and implications. Also there will be later discussions among our colleagues on the Judiciary Committee and in the Senate, so that a composite judgment may be formulated.

It may be unrealistic to assume that both bills will be viewed with equal favor by all, but it should not be too much to hope that the task of seeking a common, acceptable ground upon which to enact a law will be performed with good faith and fairness. It is in that spirit that I join with the Senator from North Carolina, and in that spirit also that I accept his joining with me in my offering of the bill of the Department of Justice.

Mr. President, I have long been concerned with the need to protect the rights of privacy of the citizens of this country and to guarantee that such rights are provided for in the operation of criminal justice information systems. I have been particularly concerned with insuring that criminal justice records are complete and accurate and that the exchange of such records is accomplished in a manner which safeguards the rights of citizens while, at the same time, providing for the legitimate needs of the criminal justice system and of the society which it serves.

In 1970 I supported an amendment offered by Senator MATHIAS to the Omnibus Crime Control and Safe Streets Act of 1968 to require the Law Enforcement Assistance Administration to submit recommendations for legislative action which would assist in promoting the integrity and accuracy of criminal justice data and would insure that the collection, dissemination, and processing of such information in criminal justice systems would be designed to provide maximum protection for the constitutional rights of all persons covered by such systems. In the 92d Congress I introduced the Criminal Justice Information System Security and Privacy Act of 1971, S. 2546, which was the LEAA response to Senator MATHIAS' amendment.

In the first session of this Congress, Senator MCCLELLAN and I supported and supplemented the amendment by the distinguished Senator from Massachusetts (Mr. KENNEDY) to the Crime Control Act of 1973 which required LEAA to issue regulations to insure as far as practicable the completeness and accuracy of information contained in LEAA-funded criminal justice systems. The amendment, section 524(b) of the Crime Control Act, limited the dissemination of criminal justice information in LEAA-funded systems to legally authorized needs and required that individuals have access to their records in order to insure that information contained about them in the system is accurate and complete. I stated at that time that additional legislation would be forthcoming which would supplement and complement that amendment to the Safe Streets Act.

The Criminal Justice Information Systems Act of 1974 which I introduce today applies to all criminal justice information systems funded in whole or in part by the Federal Government. It also applies to all interstate criminal justice information systems, and to the extent that a State or local system exchanges information with a federally funded or interstate system such system would also be subject to the provisions of this legislation.

The Criminal Justice Act applies to both manual and automated information systems. It deals comprehensively with the dissemination of arrest records and the access and use of all criminal justice information. Strong provisions are provided for an individual to review information contained in the system for the purpose of challenge or correction. Criminal justice agencies contributing criminal offender record information to a criminal justice information system are required to supply accurate and complete data and must regularly and accurately revise such data to include dispositional information.

The bill provides that criminal intelligence data must be kept separately from criminal offender record information and may only be used for a criminal justice purpose.

Provision is also made in this act for the sealing of criminal offender record information under specified circumstances. Dissemination and use of criminal justice information for noncriminal justice purposes is severely limited. The bill sets forth administrative sanctions and civil and criminal penalties for the violation of the provisions.

There are many similarities between the Criminal Justice Information Systems Act of 1974 and Senator ERVIN's bill, the Criminal Justice Information Control and Protection of Privacy Act of 1974 which I am cosponsoring today.

Both bills reflect much of the work of the LEAA-funded programs, Project SEARCH—System for Electronic Access and Retrieval of Criminal Histories—which in 1970 developed strong regulations for protecting the security and privacy of criminal justice systems. They also reflect many of the recommendations of the National Advisory Commission on Criminal Justice Standards and Goals as set forth in its commendable task force report on criminal justice systems. The security and privacy controls of the Federal Bureau of Investigation and its National Crime Information Center are also reflected in the bills.

Both bills recognize the harm which can occur through the exchange of inaccurate or incomplete records and provide methods to insure that data collected will be both accurate and complete. Each allows an individual to review a criminal offender record concerning himself for the purpose of correction.

Both bills contain requirements for sealing of records where an individual has been free from the jurisdiction of a criminal justice agency for a set period of time and the information is unlikely to provide a reliable guide to the behavior of the individual. Each requires annual public notice by a criminal justice agency of the existence and character of its automated systems.

Both bills set forth dissemination limitations and provide for administrative sanctions, civil and criminal remedies for violation of the acts.

It is because of these similarities and because of our traditional interest in achieving bipartisan support for legislation that I am cosponsoring Senator ERVIN's bill and Senator ERVIN is cosponsoring my bill.

Senator ERVIN has done a great service in providing us with this bill, as has the Department of Justice, through its Attorney General and his very dedicated staff, in compiling and formulating the bill which I have introduced. This is a complicated area, and the more ideas we have to consider the better able we will be to provide the best possible legislation. In keeping with this spirit of cooperation and bipartisanship, I look forward to the development and progress which the hearings which have been announced will produce, and which later developments will also follow.

The steadily increasing capability of the criminal justice system for gathering, processing and transmitting information requires prompt attention to the issues of system security and individual privacy. Criminal justice has a valid need for more and better information but there is an equally valid need to insure that this information is kept in a secure manner where it cannot be destroyed and to guarantee that the constitutional rights of citizens who have their records entered in this system are fully protected. There must be a balancing between all of these interests. The legislation introduced today seeks to strike that balance.

Hearings on these bills and on any other pertinent bills will be forthcoming soon, and I hope that as a result thereof we can put together a mutually acceptable bill in a reasonable time.

It is my further hope that in setting these hearings for a specific day and specific hour, some accommodation will be made for other committees, subcommittees, of the Committee on the Judiciary as well as others, because, while all of us must sacrifice the opportunity, in some instances, to follow through on some hearings on this particular subject, I am sure that we would all like to be present at as many of those hearings as possible.

Mr. President, I ask unanimous consent that the text of my bill, along with the letter of transmittal from the Attorney General and his section-by-section analysis, be printed in the RECORD immediately following my remarks.

There being no objection, the bill, the section-by-section analysis and letter of transmittal were ordered to be printed in the RECORD, as follows:

S. 2964

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Criminal Justice Information Systems Act of 1974."

FINDINGS AND PURPOSE

SEC. 2. (a) The exchange of criminal justice information including criminal offender record information or summaries of the criminal records of individuals, between Federal and State criminal justice agencies or between criminal justice agencies located in different States is a useful and proper aid to law enforcement. However, such exchange and the handling of the information must be accomplished in a manner which safeguards the interests of the individuals to whom the information refers.

(b) Particular risks, from the standpoint of the individual, may be presented when criminal justice information is used for a purpose not related to criminal justice. No such use should be permitted unless it is clearly necessary and is justified on the basis of weighing the interests of the individual (including the right of privacy, procedural rights, and access to employment) against the needs of government or of society.

(c) Enforcement of criminal laws is primarily the responsibility of State and local governments. However, Federal regulation of the criminal justice information systems which are covered by this Act is appropriate because of the Federally connected or interstate nature of those systems. This Act is based upon the powers of Congress—

(1) to place reasonable conditions upon the receipt of Federal grants or other Federal services or benefits,

(2) to regulate use of the means of interstate communication, and

(3) to enforce the Due Process and Equal Protection Clauses of the Fourteenth Amendment.

DEFINITIONS

SEC. 3. For the purpose of this Act—

(a) "Criminal justice information system" means a system, including the equipment, facilities, procedures, agreements, and organizations, utilized for the collection, processing, preservation or dissemination of criminal justice information.

(b) "Automated system" means a criminal justice information system that utilizes electronic computers or other automatic data processing equipment, as distinguished from a system in which all operations are performed manually.

(c) "Criminal offender record information" means information contained in a criminal justice information system, compiled by a criminal justice agency for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status.

(d) "Criminal intelligence information" means information compiled by a criminal justice agency for the purpose of criminal investigation, including reports of informants and investigators, contained in a criminal justice information system and associated with an identifiable individual. The term does not include criminal offender record information.

(e) "Criminal offender processing information" includes all reports identifiable to an individual compiled at any stage of the criminal justice process from arrest or indictment through release from supervision. This term does not include criminal intelligence information.

(f) "Criminal justice information" means criminal offender record information, criminal intelligence information and criminal offender processing informaiton.

(g) "Criminal justice" means any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon or parole authorities.

(h) "Criminal justice agency" means a public agency or component thereof which performs as its principal function a criminal justice activity.

(i) "Interstate system" means a criminal justice information system which is used for the transfer of criminal justice information between criminal justice agencies located in two or more States.

(j) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(k) "Attorney General" means the Attorney General of the United States or his designee.

(l) "Sealing" means the closing of a record so that the information contained in the record is available only (1) in connection with review pursuant to section 6 by the individual or (2) on the basis of a court order or a specific determination of the Attorney General.

COVERAGE

SEC. 4. (a) This Act applies to any criminal justice information system which is—

(1) operated by the Federal Government,

(2) operated by a State or local government and funded in whole or in part by the Federal Government,

(3) an interstate system, or

(4) operated by a State or local government and engaged in the exchange of criminal justice information with a system covered by paragraphs (1), (2), or (3): Provided that a system described only by paragraph (4) shall be subject to this Act only to the extent of its participation with a system described by paragraphs (1), (2), or (3).

(b) This Act applies to criminal justice information obtained from a foreign government or an international agency to the extent that such information is contained in a criminal justice information system subject to this Act. Whenever any criminal justice information contained in a criminal justice information system subject to this Act is provided to a foreign government or an international agency, appropriate steps should be taken to assure that such information is used in a manner consistent with the provisions of this Act.

(c) The provisions of this Act do not apply to lists or systems utilized by criminal justice agencies for the sole purpose of identifying or apprehending fugitives or wanted persons.

ACCESS AND USE

SEC. 5. (a) The provisions of this section apply to any criminal justice information system subject to this Act and to any agency or person who, directly or indirectly, obtains criminal justice information from such a system.

(b) Direct access to information contained in a criminal justice information system subject to this Act shall be available only to authorized officers or employees of a criminal justice agency.

(c) (1) Except as provided in paragraphs (2) and (3), criminal intelligence information may be used only for a criminal justice purpose, and only where need for the use has been established in accord with regulations issued by the Attorney General.

(2) Criminal intelligence information may be used for a purpose not related to criminal justice if the Attorney General determines, with regard to the particular case or class of cases, that such use is necessary because of reasons of national defense or foreign policy.

(3) Criminal intelligence information compiled by a criminal justice agency which is a component of a Federal, State or local agency may be made available to a non-criminal-justice component of the same agency if the information is necessary for performance of a statutory function of the non-criminal-justice component. Such information may be used by the non-criminal-justice component only in connection with performance of a statutory function.

(d) (1) Except as provided in paragraphs (2)-(4), criminal offender processing information may be used only for a criminal justice purpose, and only where need for

the use has been established in accord with regulations issued by the Attorney General.

(2) Particular criminal offender processing information may be made available to the individual to whom the information refers, pursuant to a court order or a Federal or State statute or regulation.

(3) Criminal offender processing information may be made available to qualified persons for research related to criminal justice under procedures designed to assure the security of the information released and the privacy of individuals to whom the information refers.

(4) Criminal offender processing information may be used for a purpose not related to criminal justice if such use is expressly authorized by a court order of Federal or State statute. The Attorney General shall determine, with regard to the particular case or class of cases, whether such use is expressly authorized by statute, and his determination shall be conclusive.

(e) (1) Criminal offender record information may be used for criminal justice purposes or for other purposes which are expressly provided for by Federal statute or Executive order or State statute. The Attorney General shall determine, with regard to the particular case or class of cases, whether such use is expressly provided for by statute or by Executive order, and his determination shall be conclusive.

(2) Criminal offender record information may be made available, pursuant to section 6, to the individual.

(3) Criminal offender record information may be made available to qualified persons for research related to criminal justice under procedures designed to assure the security of the information released and the privacy of individuals to whom the information refers.

(f) Any agency operating a criminal justice information system subject to this Act shall maintain records with regard to—

(1) requests from any other agency or person for criminal justice information. Such records shall include:

(A) regarding any request for use for a criminal justice purpose, the identity of the requester, the nature of the information provided and pertinent dates; and

(B) regarding any request for use for a non-criminal-justice purpose, the identity of the requester, the nature, purpose and disposition of the request, and pertinent dates.

(2) the source of criminal offender record information: *Provided*, That regulations of the Attorney General may provide for exceptions with regard to the source of identifying data.

REVIEW OF CRIMINAL OFFENDER RECORD INFORMATION BY THE INDIVIDUAL

SEC. 6. (a) Any individual who complies with applicable regulations shall be entitled to review criminal offender record information regarding himself contained in any criminal justice information system subject to this Act, and to obtain a copy of the information for the purpose of challenge or correction.

(b) Each Federal agency which operates a criminal justice information system and each State shall adopt regulations to implement this section. Such regulations shall (1) require that an individual making such a request verify his identity by fingerprints or other specified means, (2) explain the procedures for making such requests and performing such review, including such matters as time, place and fees, and (3) provide for the waiver, in appropriate cases, of any applicable fees.

(c) Except with regard to national defense or foreign policy cases, or with regard to the appointment of a judge or a civil officer, which appointment is subject to the advice and consent of the Senate, when criminal offender record information is requested, in accord with paragraph (5) (e) (1), for a purpose not related to criminal justice, the criminal justice agency to which the request is made shall require the requester to notify the individual that criminal offender record information concerning him is being requested, and that he has a right to review his record for the purpose of challenge or correction.

(d) No individual who, in accord with subsection (a) or (c), obtains a copy of criminal offender record information regarding himself may be required or requested to show or transfer that copy to any person or agency.

(e) If, after review of information obtained pursuant to subsection (a) or (c), the individual disputes its accuracy or completeness, he may apply for correction or revision to the agency responsible for original entry of the allegedly incomplete or inaccurate information. When correction or revision is warranted, the responsible agency shall immediately make the necessary correction or revision and take appropriate steps to have the correction or revision made with respect to all criminal justice information systems containing the information.

(f) In the event that an individual is dissatisfied with the decision of a criminal justice agency with respect to his request for correction or revision of information, the individual shall be afforded administrative review in accord with applicable regulations.

(g) If an individual is dissatisfied with the final administrative decision, he may obtain judicial review of that decision by bringing an action pursuant to subsection 14(a).

ACCURACY AND COMPLETENESS OF CRIMINAL OFFENDER RECORD INFORMATION

SEC. 7. (a) Any criminal justice agency which contributes criminal offender record information to a criminal justice information system subject to this Act shall assure that the information it contributes is accurate and complete and that it is regularly and accurately revised to include dispositional and other subsequent information.

(b) All Federal, State or local criminal justice agencies, including courts and correctional authorities, shall take the steps necessary to achieve compliance with subsection (a).

DISSEMINATION OF ARREST RECORDS

SEC. 8. (a) This section applies to any criminal justice information system subject to this Act and to any agency or person who, directly or indirectly, obtains criminal offender record information from any such system.

(b) No information relating to an arrest may be disseminated without the inclusion of the final disposition of the charges if a disposition has been reported. Any agency or person requesting or receiving information relating to an arrest from a system subject to this Act shall use such information only for the purpose of the request. Subsequent use of the same information shall require a new inquiry of the system to assure that it is up-to-date.

(c) Except as provided in subsection (d), criminal offender record information concerning the arrest of an individual may not be disseminated or used for a non-criminal-justice purpose if—

(1) the individual is acquitted of the charge for which he was arrested,

(2) the charge is dismissed,

(3) a determination to abandon prosecution of the charge is made by the prosecuting attorney, or

(4) an interval of one year has elapsed from the date of the arrest and no final disposition of the charge has resulted and no active prosecution of the charge is pending: *Provided*, that the one-year period does not include any period during which the individual is a fugitive.

(d) The prohibition set forth in subsection (c) shall not apply—

(1) when the Attorney General determines, with regard to the particular case or class of cases, for reasons of national defense or foreign policy it should not apply,

(2) with regard to the appointment by the President of a judge or a civil officer whose appointment is subject to the advice and consent of the Senate,

(3) with regard to use, pursuant to paragraph (5) (e) (3), for research purposes,

(4) with regard to use, pursuant to subsection (6) (a) or (c), by the individual for adjudication of a claim that the information is inaccurate or incomplete,

(5) where a court order specifically provides otherwise, or

(6) where a Federal statute expressly provides that the prohibition shall not apply.

SEALING OF CRIMINAL OFFENDER RECORD INFORMATION

SEC. 9. (a) Criminal offender record information shall be sealed in accord with the requirements of a court order, a Federal or State statute, or regulations issued by the Attorney General, when appropriate notification is provided by the agency directly responsible for compliance with the order, statute, or regulation.

(b) The regulations shall, as a minimum, provide for the sealing of criminal offender record information regarding an individual who has been free from the jurisdiction or supervision of any criminal justice agency for—

(1) a period of seven years if the individual has previously been convicted of an offense for which imprisonment in excess of one year is permitted under the laws of the jurisdiction where the conviction occurred,

(2) for a period of five years if the individual has previously been convicted of an offense for which the maximum penalty is not greater than imprisonment for one year under the laws of the jurisdiction where the conviction occurred, or

(3) for a period of five years following an arrest if no conviction of the individual occurred during that period, no prosecution is pending at the end of that period, and the individual is not a fugitive.

(c) (1) The regulations may exempt from full compliance with the requirements of this section criminal justice information systems for which full compliance is not feasible because of the manual nature of the systems.

(2) The regulations shall set forth procedures regarding access to a sealed record (A) in connection with review pursuant to section 6 by the individual or (B) on the basis of a court order or (C) a specific determination of the Attorney General.

PRECEDENCE OF STATE LAWS

SEC. 10. Nothing in this Act is to be construed to diminish greater rights of privacy or protection provided by a State law or regulation governing use, updating, or sealing of records in that State's criminal justice information system. Use of information in interstate systems or the use of information obtained through interstate transfer shall be governed solely by this Act and implementing regulations.

SECURITY OF CRIMINAL JUSTICE INFORMATION SYSTEMS

SEC. 11. (a) The security of information in a criminal justice information system subject

to this Act shall be assured by management control by a criminal justice agency.

(b) All criminal justice information systems subject to this Act shall meet security standards promulgated by the Attorney General to guard against unauthorized access to data contained in the systems. These standards will include, but not be limited to—

(1) Implementation, operation and management control of criminal justice information systems.

(2) System design standards which take maximum advantage of security provided by existing technology.

(3) Physical security standards for the system facility and associated telecommunications networks.

(4) Administrative procedures for gaining access to data, safeguarding data and removing of data.

(c) The Attorney General shall provide for a continuous review and periodic audits of the operations of criminal justice information systems to assure that there is full compliance with the standards issued pursuant to this section and that appropriate corrective actions and sanctions are promptly invoked when required.

OPERATING PROCEDURES

SEC. 12. (a) All criminal justice information systems subject to this Act shall include operating procedures which are consistent with the regulations established and promulgated by the Attorney General and at a minimum shall—

(1) include a program of verification and audit to insure that criminal offender record information is regularly and accurately updated,

(2) limit access and dissemination of criminal justice information in accordance with the provisions of this Act,

(3) provide an administrative review mechanism for challenges by individuals to the accuracy or completeness of their records,

(4) Undertake an affirmative action program for the training of system personnel,

(5) require a complete and accurate record of access and use made of any information in the system including the identity of all persons and agencies to which access has been given, consistent with section 5(f).

(b) Each agency which operates an automated criminal justice information system subject to this Act shall publish notice at least once a year of

(1) its existence,

(2) the nature of the system,

(3) policies regarding storage, duration of retention and dissemination,

(4) procedures whereby an individual can review criminal offender record information regarding himself,

(5) the title, name and business address of the person immediately responsible for the system.

With regard to a system operated by the Federal Government, such notice shall be published in the Federal Register.

(c) Any agency operating or participating in a criminal justice information system subject to this Act may be required to provide periodic reports to the Attorney General.

ADMINISTRATIVE SANCTIONS

SEC. 13. (a) In the event that a criminal justice agency (1) obtains information from a criminal justice information system subject to this Act and uses or disseminates that information in a manner which violates this Act or regulations issued by the Attorney General, or (2) fails to provide dispositional information required by subsection 7(a), the agency may be denied access to criminal justice information systems subject to this Act.

(b) An agency or person, other than a criminal justice agency, who obtains criminal offender record information and uses that information in violation of this Act or regulations issued by the Attorney General may be denied the use of criminal offender record information subject to this Act.

(c) Procedures for implementing this section shall be set forth in regulations issued by the Attorney General. The regulations shall provide that no sanction may be imposed pursuant to subsection (a) until the Attorney General or, where appropriate, a State official has (1) provided notice of the alleged violation to the criminal justice agency in question, (2) determined that compliance cannot be secured by voluntary means, and (3) determined, after opportunity for hearing, that substantial or repeated violation of this Act or regulations issued by the Attorney General has occurred.

CIVIL AND CRIMINAL REMEDIES

SEC. 14. (a)(1) To obtain judicial review, pursuant to subsection 6(g), of a final administrative decision, an individual may bring a civil action against the responsible agency.

(2) An individual with respect to whom criminal justice information has been maintained, disseminated or used in violation of this Act or implementing regulations may bring a civil action against the individual or agency responsible for the alleged violation. If relief is sought against both the individual and the agency responsible for the alleged violation, such relief shall be sought in a single action.

(b)(1) If a defendant in an action brought under subsection (a) is an officer or employee or agency of the United States, the action shall be brought in an appropriate United States district court.

(2) If the defendant or defendants in an action brought under subsection (a) are private persons or officers or employees or agencies of a State or local government, the action may be brought in an appropriate United States district court or in any other court of competent jurisdiction.

(c) The district courts of the United States shall have jurisdiction over actions described in subsection (b), without regard to the amount in controversy.

(d) A prevailing plaintiff in an action brought under subsection (a) may be granted equitable relief, including injunctive relief, and actual damages, and may be awarded costs and reasonable attorney fees. In appropriate cases, a prevailing plaintiff may also be awarded exemplary damages.

(e) Any person who disseminates or uses criminal justice information knowing such dissemination or use to be in violation of this Act or any applicable regulations shall be fined not more than $10,000 or imprisoned for not more than one year, or both.

(f) Good faith reliance upon the provisions of this Act or of applicable law governing maintenance, dissemination, or use of criminal justice information, or upon rules, regulations, or procedures prescribed or approved by the Attorney General shall constitute a complete defense to a criminal action brought under this Act. With respect to damages, such reliance shall constitute a complete defense for an individual or an agency in a civil action brought under this Act. Such reliance shall not constitute a defense with respect to equitable relief.

COMPLIANCE WITH ACT

SEC. 15. Any State or local agency which operates or participates in a criminal justice information system subject to this Act shall comply with this Act and with regulations issued by the Attorney General and shall be deemed to have consented to the bringing of actions pursuant to subsection 14(a).

REGULATIONS OF THE ATTORNEY GENERAL

SEC. 16. After appropriate consultation with Federal and State agencies which operate or use criminal justice information systems, the Attorney General shall issue regulations implementing this Act.

AUTHORIZATION

SEC. 17. There are hereby authorized to be appropriated such funds as may be necessary for the Attorney General to implement this Act.

EFFECTIVE DATE

SEC. 18. This Act shall become effective one year after the date of enactment, except that section 17 shall become effective upon the date of enactment.

CRIMINAL JUSTICE INFORMATION SYSTEMS ACT OF 1974—SECTION-BY-SECTION ANALYSIS

Sec. 1 is the enactment and title clause.

Sec. 2. Findings and Purpose—

Subsection (a) refers to the usefulness of exchanging criminal justice information between Federal and State criminal justice agencies and between States, but points out the need to safeguard the rights of affected individuals.

Subsection (b) states that criminal justice information is to be used for a non-criminal-justice purpose only when such use is justified on the basis of weighing the interests of the individual against the needs of government or society.

Subsection (c) sets forth the constitutional basis for the Act.

Sec. 3. Definitions—

Subsection (a). "Criminal justice information system". This definition sets forth the basis for the coverage of the Act. The term refers to systems, automated or manual, for the collection, processing, preservation or dissemination of criminal justice information.

Subsection (b). "Automated system" is defined as a criminal justice information system which utilizes electronic computers or other automatic data processing equipment. This term applies where part of the system is automated and part manual, for example, a system which stores criminal offender record information in a computer file.

Subsection (c). "Criminal offender record information" includes (1) the factual summary of events of each formal stage of the criminal justice process: notations of arrest, the nature and disposition of criminal charges, sentencing, confinement, parole and probation status, formal termination of the criminal justice process as to a charge or conviction and (2) physical and other identifying data.

Subsection (d). "Criminal intelligence information" is defined as information which is compiled by criminal justice agencies for purposes of criminal investigation and which is indexed under an individual's name or otherwise associated with an individual. Such information may include reports of informants or investigators. This term does not include criminal offender record information, and any agency which maintains both criminal intelligence information and criminal offender record information must keep the two types of information separate. However, accounts of arrests or convictions may be expected in investigative reports, and there is no intention to exclude such non-systematic references to offender record information from criminal intelligence files.

Subsection (e). "Criminal offender processing information" is defined as detailed reports (as opposed to notations), identifiable to an individual, and compiled by any criminal justice agency for the purpose of processing the individual from the time of arrest to the time of release from supervision. This would include background reports on in-

dividual offenders such as arrest reports, pre-sentence reports, etc.

Subsection (f). "Criminal justice information" is defined to include criminal offender record information, criminal intelligence information, and criminal offender processing information. Files that are not maintained in an individually identifiable manner, such as chronologically ordered police blotters and court dockets, are not considered within the scope of the Act.

Subsection (g). "Criminal justice" is defined to mean any activity pertaining to the enforcement of criminal laws. This term includes police efforts to prevent, control or reduce crime or to apprehend criminals. Also included are activities of prosecutors, courts and corrections, probation, pardon or parole authorities.

Subsection (h). "Criminal justice agency" means a public agency, Federal, state or local, whose principal function is the performance of activities pertaining to criminal justice. The definition includes a "component" of a public agency if the principal function of the component is performing activities relating to criminal justice. For example, a unit of the Internal Revenue Service which has as its principal function investigation of criminal violations of the tax laws would be a "criminal justice agency" even though the Internal Revenue Service as a whole would not come within that definition.

Subsection (i). "Interstate system" is defined as a system for the transfer of criminal justice information between criminal justice agencies located in two or more states.

Subsection (j). "State" is defined to include the District of Columbia, Puerto Rico and the territories or possessions of the United States.

Subsection (k). "Attorney General" is defined as the Attorney General of the United States or his designee.

Subsection (l). "Sealing" is defined as the closing of a record so that information will no longer be available except for review by an individual to whom the record pertains or by court order, or a specific determination of the Attorney General.

Sec. 4. Coverage—

Subsection (a) specifies the type of systems which are covered by this Act. Such systems include those operated by the Federal Government, funded in whole or in part by the Federal Government, an interstate system and any system which is engaged in the exchange of criminal justice information with the above systems to the extent of such participation.

Subsection (b) provides that the Act applies to criminal justice information obtained from a foreign government or an international agency to the extent that such information is contained in a system subject to this Act. When such information is provided to a foreign government or an international agency, use of the information by the foreign government or international agency should be consistent with this Act.

Subsection (c) exempts lists or systems used by criminal justice agencies for the purpose of identifying or apprehending fugitives or wanted persons.

Sec. 5. Access and Use—

Subsection (a) sets forth that the provisions of this section apply to any criminal justice information system subject to this Act and to any agency or person who obtains information from such a system either directly or indirectly.

Nothing in the Act is intended to prevent the public release of general information concerning an offense, a specific arrest, indictment, or disposition, within a reasonable time after the event has occurred.

Subsection (b) limits direct access to criminal justice information systems to authorized officers and employees of criminal justice agencies. Standards and procedures for determining what officers and employees are "authorized" are to be prescribed by regulations. All information permitted for non-criminal justice purposes must be obtained through a criminal justice agency.

Subsection (c) provides that criminal intelligence information may only be used for a criminal justice purpose (except as stated below) and that need for such use must have been established in accord with regulations issued under the Act. Thus, an agency seeking such information has the burden of establishing its entitlement and systems are to be designed so that such information is not routinely obtainable by the requesting agency. The provision allows criminal intelligence information to be used for non-criminal justice purposes if the Attorney General determines in a particular case or class of cases that use is necessary for reasons of national defense or foreign policy.

Subsection (d) provides that criminal offender processing information may be used only for a criminal justice purpose (except as stated below) and only where need has been established in accord with regulations to be issued under this Act. Pursuant to a court order, Federal or state statute or regulation particular criminal offender processing information concerning an individual may be made available to him. Under procedures which shall assure security and privacy of such information, information may also be made available to qualified persons for research related to criminal justice. Criminal offender processing information may be made available for a non-criminal justice purpose if such use is expressly provided for in a Federal or State statute.

Subsection (e) relates to use of criminal offender record information and provides that such information may be used for criminal justice purposes. That is, one criminal justice agency may obtain criminal offender record information from another agency for use with regard to the former's criminal justice responsibilities.

Criminal offender record information may be used for a purpose not related to criminal justice if such use is expressly provided for in a Federal statute or executive order or in a state statute. A municipal ordinance is not a sufficient basis unless the ordinance implements or is a type expressly authorized by a state statute dealing with use of criminal offender record information.

The determination whether a statute ro executive order "expressly provides for" such use shall be made by the Attorney General. His determinations shall be conclusive.

The provisions of Subsection (e) allowing for non-criminal justice uses of offender record information are subject to the further limits on arrest records contained in Section 8.

One reason for the delayed effective date of this statute is the hope that it will provide an opportunity for states and the Federal Government to carefully review the statutory authorizations that now exist.

Criminal offender record information may also be made available to qualified persons for research pertaining to criminal justice. Such use is to be governed by regulations which shall establish procedures to assure the security of the information which is released and to protect the privacy of the individuals to whom the information relates.

Subsection (f) requires that records must be maintained for each criminal justice information system with regard to (1) requests for use of criminal justice information and (2) the source of criminal offender record information.

Sec. 6. Review of Criminal Offender Record Information by the Individual—

Subsection (a) requires that an individual, after complying with applicable regulations, be entitled to review criminal offender record information regarding himself and obtain a copy for the purpose of challenge or correction. This requirement does not apply to either criminal intelligence information or criminal offender processing information. It is intended that the regulations will contain procedures to allow an attorney to act on behalf of an individual, and to facilitate individual review of records maintained at geographically distant points.

Subsection (b) provides that each Federal and State agency adopt regulations to implement this section.

Subsection (c) requires that whenever criminal offender record information is requested for a non-criminal justice purpose, the requester must notify the individual to whom the information refers that information is being requested concerning him, and that he has a right to review the record for purposes of challenge or correction. The regulations will contain procedures designed to assure that such notice is given prior to release of the information in order to minimize the chances for release of inaccurate information.

Subsecion (d) prohibits any agency or person from requiring or requesting an individual to show or transfer a copy of this information regarding himself.

Subsection (e) states that an individual who exercises his right of review and who disputes the accuracy or completeness of the information may apply to have the information corrected or supplemented. The application is to be made to the agency (or agencies) responsible for the allegedly inaccurate or incomplete information. Normally the individual applying for corrective action must apply to the arresting agency or to the prosecutive agency, court or correctional institution, where appropriate. The responsible agency will normally not be the agency maintaining a statewide or national file.

Any necessary corrections or revisions are to be made by the responsible agency as soon as possible and are to be disseminated to all past recipients of the erroneous or incomplete information.

Subsection (f) requires that any individual who is not satisfied with the disposition of his request for correction or revision be afforded administrative review.

Subsection (g) gives a right of judicial review to any individual who is not satisfied with the decision resulting from final administrative review.

Sec. 7. Accuracy and Completeness of Criminal Offender Record Information—

Subsection (a) requires a criminal justice agency contributing criminal offender record information to a system subject to this Act to assure that the information which it contributes is accurate, complete and regularly revised to include dispositional and other subsequent information.

Subsection (b) states that all criminal justice agencies, covered by this Act, must take steps necessary to achieve compliance with subsection (a). Criminal justice agencies include courts and correctional authorities.

Sec. 8. Dissemination of Arrest Records—

Subsection (a) states the coverage of this section. The section applies to any criminal justice information system subject to this Act and to any agency or person who directly or indirectly obtains criminal offender record information from such a system.

Subsection (b) restricts dissemination of an arrest record that does not include final

disposition if a final disposition has been reported by the contributing criminal justice agency. Each use of a record shall require an inquiry of the system to assure that the information is up-to-date and accurate.

Subsection (c) prohibits dissemination of an arrest record for non-criminal justice purposes if there is an acquittal, dismissal, abandonment of prosecution or an interval of one year has elapsed from date of arrest and no active prosecution is pending. However, if within this one-year period the individual is a fugitive, the time period during which he is a fugitive is excluded. Or, if a person is tried on only one of several charges, and when sentenced, the other charges are held open until the completion of the sentence given, this would be interpreted as "active prosecution still pending".

Subsection (d) exempts from the above prohibition (1) cases where the Attorney General determines that for national defense or foreign policy reasons it should not apply, (2) with regard to the appointment of certain officers by the President, (3) use for research purposes under section 5(e)(3), (4) use pursuant to review of a record by an individual, or adjudication of a claim that the information is inaccurate or incomplete, (5) where a court order specifically provides otherwise, or (6) where a Federal statute expressly provides otherwise.

Sec. 9. Sealing of Criminal Offender Record Information—

Subsection (a) requires that criminal offender record information be sealed under specified circumstances.

Subsection (b) requires that regulations provide at a minimum the sealing of criminal offender record information when specified periods of time have elapsed and an individual has been free from the jurisdiction or supervision of any criminal justice agency. The regulations will establish standard procedures whereby the State will provide information as to the maximum penalty for the particular offense when notation of the sentence is entered into the system.

Subsection (c) allows the regulations to exempt particular systems from full compliance with the sealing requirements where because of the manual nature of such systems, such full compliance would not be feasible. In particular, it is anticipated that records predating the effective date of this Act will be considered for sealing on a one-by-one basis as they are requested for use or as they are coded for conversion to automated systems.

The regulations must also set forth procedures for access. Where access to a sealed record is allowed in connection with review by the individual, on the basis of a court order, or a specific determination of the Attorney General, regulations must set forth procedures to be followed.

Sec. 10. Precedence of State Laws—

This section specifies that where a particular State has a law or regulation which affords an individual rights of privacy which are designed to protect the interests of individuals who are the subject of information in the State's criminal justice information system, that such a law or regulation would not be in conflict with this Act. A State may provide rights of privacy or protection for information in its system greater than those set forth in this Act and such provisions would govern in that State's criminal justice information systems.

Sec. 11. Security of Criminal Justice Information Systems—

This section is designed to minimize the possibility of unauthorized disclosure by setting forth the means by which such systems shall be operated. The security of information in a system subject to this Act must be assured by management control by a criminal justice agency. Also, such systems must meet security standards promulgated by the Attorney General to guard against unauthorized access to data within them.

In addition, the Attorney General is directed to provide for a continuous review and periodic audits of the operations of these systems to assure full compliance with the standards issued pursuant to this section.

Sec. 12. Operating Procedures—

Subsection (a) requires that all criminal justice information systems subject to this legislation must include specified minimum operating procedures which are consistent with the regulations established and promulgated by the Attorney General.

Subsection (b) requires an agency which operates an automated criminal justice information system subject to this Act to publish once a year notice of the existence, nature, and procedures governing the system. If such a system is operated by the Federal Government this notice shall be published in the Federal Register.

Subsection (c) allows the Attorney General to require any agency participating in a criminal justice information system subject to this legislation to provide periodic reports.

Sec. 13. Administrative Sanctions—

Subsection (a) provides that a criminal justice agency may be denied access to criminal justice information systems which are subject to this Act if such an agency (1) obtains information from such a system, and uses or disseminates that information in violation of this Act or the regulations issued pursuant to it, or (2) such agency fails to provide dispositional information required by the Act.

Subsection (b) provides that any person or agency, other than a criminal justice agency, may be denied the use of criminal offender record information if such person or agency uses such information in violation of this Act or regulations issued pursuant to it by the Attorney General.

Subsection (c) states that procedures regarding use of administrative sanctions are to be set forth in regulations of the Attorney General.

Sec. 14. Civil and Criminal Remedies—

Subsection (a)(1) permits an individual who is dissatisfied with the final administrative decision regarding his request for correction and revision of criminal offender record information which pertains to him, to bring a civil action against the responsible agency.

Subsection (a)(2) permits an individual with respect to whom criminal justice information has been maintained disseminated or used in violation of the Act or regulations issued pursuant to it, to bring a civil action against the responsible person or agency.

Subsection (b)(1) requires that such civil actions must be brought in the appropriate United States District Court if a defendant is an officer, employee, or agency of the United States.

Subsection (b)(2) provides that if the defendants in such civil actions are private persons, or officers, employees or agencies of a state or local government, such actions may be brought in an appropriate United States District Court or any other court of competent jurisdiction.

Subsection (c) provides that the district courts of the United States have jurisdiction over such civil suits without regard to the amount in controversy.

Subsection (d) provides that a prevailing plaintiff in such civil actions may be granted equitable relief, damages, costs, and reasonable attorney fees. Exemplary damages may also be awarded when appropriate.

Subsection (e) provides criminal penalties for dissemination and use of criminal justice information which is in violation of the Act and any applicable regulations issued pursuant to it. It is assumed that forgeries or other unauthorized alterations of records subject to this Act are punishable under 18 U.S.C. § 1001 et. seq., and similar provisions of law.

Subsection (f) provides an individual or agency with a complete defense against any civil or criminal action (except an action for equitable relief) when such an individual or agency acts in good faith relying upon the provisions of the Act or on applicable law governing the maintenance, dissemination, or use of criminal justice information, or upon rules, regulations, or procedures prescribed or approved by the Attorney General.

The defense of "good faith" is intended to apply only where one innocently followed the rules without notice that there was a claim of error or invalidity. The test is an objective one and not the actual state of mind of the individual. Good faith requires the exercise of reasonable diligence to learn the truth when one is put on inquiry.

It is anticipated that the remedies contained in this section will be applied consistent with the provisions of the First Amendment to the Constitution.

Sec. 15. Compliance with Act—.

This section would require any state or local agency which operates or participates in a criminal justice information system which is subject to the Act to comply with the Act and with the regulations issued pursuant to it by the Attorney General. Also, any such agency would be deemed to have consented to the bringing of such civil actions as authorized by the Act.

Sec. 16. Regulations of the Attorney General—

The Attorney General is required to issue regulations implementing this Act after appropriate consultation with Federal and state agencies operating or using criminal justice information systems.

Sec. 17. Authorization—

Authorizes funds for the Attorney General to implement the Act.

Sec. 18. Effective Date—

Sets the effective date of the Act to be one year after the date of enactment, except for the authorization of funds section, which would become effective the date of enactment.

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., February 5, 1974.

The VICE PRESIDENT
U.S. Senate
Washington, D.C.

DEAR MR. VICE PRESIDENT: Enclosed for your consideration and appropriate reference is a legislative proposal entitled the "Criminal Justice Information Systems Act of 1974."

This is a legislative proposal to facilitate and regulate the exchange of criminal justice information.

The proposal, I believe, has achieved an appropriate balance between the information needs of governments and the constitutional rights of persons affected by the collection and dissemination of criminal justice information. This bill is more comprehensive than the proposal originally submitted during the 92nd Congress, 1st Session, and introduced as S. 2546. This bill is applicable to any criminal justice information system which is operated by the Federal Government or is funded in whole or in part by the Federal Government. Also covered is any interstate system and any system which is engaged in the exchange of information with a Federally operated, Federally funded, or interstate system. Both automated and manual systems are covered.

Direct access to criminal justice informa-

tion systems is limited to criminal justice agencies. Criminal offender record information in a system may only be used for criminal justice purposes unless there is a Federal statute, Executive order or State statute which expressly provides for a non-criminal justice use. This would mean that criminal offender record information would be unavailable for employment or credit checks unless a statute specifically required such use.

The draft bill provides the individual with the right of review of his record for the purposes of correction. Stringent restrictions on dissemination are provided. Criminal offender record information is required to be accurate and complete and provision is made for the sealing of criminal offender record information after the passage of a stated period of years during which the individual is free from the supervision of a criminal justice system. Provision is made for administrative, civil and criminal sanctions against those who use or disseminate information in violation of the Act.

Several provisions of the bill would require changes in the current practices of some government agencies, particularly non-criminal justice agencies that have traditionally made use of criminal justice data for various purposes. The debate and action taken on this proposal should serve to clarify national policy in this area and to provide a framework for subsequent efforts which will, hopefully, bring some order and consistency to the array of statutes and regulations that are relied on for access and use to criminal justice information.

The proposed legislation reflects a strong concern for the security and privacy of data in criminal justice information systems and deals effectively with the fundamental issues involved. Its early and favorable consideration is urged.

The Office of Management and Budget has advised that there is no objection to the submission of this proposal from the standpoint of the Administration's program.

Sincerely,

_____,
Attorney General.

COMPUTERIZED CRIMINAL HISTORY DATA BANKS

Mr. ROBERT C. BYRD. Mr. President, I applaud the President's statement in the state of the Union address that individual liberties must be protected from the unwarranted invasion of computerized criminal history data banks. The Justice Department is supporting legislation that, for the first time, would place legal restrictions on local, State, and Federal crime data banks. This is a significant recognition on the part of the administration of the growing concern of the possible abuses inherent in a large computerized criminal data bank, such as the FBI's National Crime Information Center—NCIC.

According to statistics I received yesterday from the FBI, the NCIC telecommunications network had 89 control terminals at criminal justice agencies, 56 of which are computerized. In addition, all 59 FBI field offices are linked to the central computer at FBI headquarters. Through this system, information from more than 4.8 million records stored in the FBI's computer is almost immediately available to more than 6,000 police agencies. The NCIC handles more than 121,000 transactions daily.

There are over 440,000 computerized criminal histories—CCH—in the NCIC.

These statistics are increasing at an accelerated rate—during the hearings on the confirmation of L. Patrick Gray to be FBI Director, the Bureau estimated the following growth for the NCIC in the coming years: The number of records that will be contained in NCIC in 5 years will be 10.1 million and 10 years hence will be 21.7 million; the number of computerized criminal histories contained in the NCIC computer in 5 years will be 3 million and 10 years hence will be 8 million.

The anticipated growth of the NCIC adds greater urgency to the necessity for congressional action to assure strict and yet workable procedural safeguards for the system.

Both the bill introduced by Senator ERVIN and the bill introduced by Senator HRUSKA are intended to be starting points for intensive hearings to determine what safeguards are necessary to protect individual liberties and, at the same time, to allow the most effective use of the system in aiding the criminal justice system. For this reason, I have joined as a cosponsor of both bills.

I appreciate the courtesy of the Senator from North Carolina (Mr. ERVIN) and the courtesy of the Senator from Nebraska (Mr. HRUSKA) in allowing me to join as a cosponsor of both bills.

As a member of the Constitutional Rights Subcommittee of the Judiciary Committee, this has been an area of concern to me for some time. This is a difficult field in which to legislate, but it is one in which we must legislate to carefully delineate the lines beyond which such computer systems may not go. Everyone recognizes the blessings such a system may bring for our law enforcement agencies, but at the same time, we must be alert to the dangers that are inherent to such a system.

I think we in the Congress must carefully weigh the interests involved in this legislation and come forward with guidelines to be followed in the future.

Mr. MATHIAS. Mr. President, it is with a rare sense of satisfaction that we come together for introduction today of the "Criminal Justice Information Control and Protection of Privacy Act of 1974." I am pleased to join Senators ERVIN and HRUSKA and other Members of the Senate, in introducing this bill, and to also cosponsor the administration's bill on the same subject.

My satisfaction stems from finally seeing progress and sensing victory on an issue of vital importance to the survival of constitutional government in the United States. About 4 years ago, on my motion, the Senate directed the Department of Justice to prepare guidelines on the use of personal information held in data banks. This is the action just described by the distinguished Senator from Nebraska (Mr. HRUSKA.) Unhappily, the Department ignored this request and the Senate condoned the lapse. Thus, both the legislative and executive branches demonstrated shocking insensitivity to a highly sensitive subject.

Today, that unfortunate chapter is being excised from our record and we are returning to the spirit in which the Senate adopted my original proposal.

The administration merits support for its stated policy and for the attention it is drawing to the problems of privacy in our society. The President's state of the Union message, and the legislation which is being introduced today, have great significance, not only for their symbolic value but because these bills represent a genuine first step in one important facet of the privacy problem. Not to be forgotten are two Attorneys General, Elliot Richardson and William Saxbe, who are men sensitive to this issue and who deserve credit for helping to bring the Department of Justice to its present posture.

Ours has indeed become "an information-rich world" and the availability of the computer is both cause and effect of this characteristic of modern society. But the increasing sophistication of the computer means that information concerning individuals can, for the first time, be collected and stored, shared, analyzed, and brought to bear for good or ill. Alexander Solzhenitsyn saw it when he said in "Cancer Ward":

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams, then even people would loose all the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence . . . Each man constantly aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

The legislation introduced today recognizes the reality of these "threads" and attempts to reconcile the uses to which our new technology can be put with the rights of individuals. It attempts to draw the line which says how and when the individual can be fettered and how and when he shall be free. These bills do not, it should be added, deal with all problems of privacy. Many other privacy issues remain, such as the protection of fourth amendment freedoms and the problem of vast amounts of information concerning individuals presently collected and held by private entities. They do address one important facet of the problem, criminal records information shared between law enforcement agencies.

This is an issue with which I have long been concerned. I began work on this issue when I was in the House of Representatives. In the 92d Congress, I sponsored an Omnibus Criminal Justice Reform Act which, in its concern for the successful rehabilitation of the individual, acquainted me with the problems of such information. When Patrick Gray came before the Senate Judiciary Committee for confirmation, I prepared an extensive list of questions concerning the FBI's

NCIC system and its relationship to State agencies. The information elicited in those questions and in similar questions propounded to FBI Director Clarence Kelley, during the course of his confirmation hearings will, I am sure, be useful to the work of the Senate.

In November, I joined Senator ERVIN in introducing legislation which would have clarified what is, in my view the currently ambiguous authority of the FBI to disseminate information in its files.

The NCIC and participating State systems constitute a vast network for the exchange of information between the law enforcement agencies of the States and the Federal Government and among the States. This system has enormous potential for increasing the capability of law enforcement. When the system is fully operational, each individual police officer could instantaneously have information from all over the Nation concerning suspects at his finger-tips simply by contacting his local computer terminal. Such contact might even be made from a patrol car. This tool can be extremely valuable to police and other law enforcement officials faced with problems which do not respect jurisdictional lines or, in our modern society, distance.

But as with so many technological wonders of our age, this miracle for communicating information raises new problems which must be addressed. In this case, the problems concerning using this system in a way that protects constitutional liberties and civil rights, including the right of privacy.

With the introduction of this legislation today, the Senate is undertaking to resolve a number of issues with respect to criminal history information. These important issues are the classification of types of information which can be collected, the uses to which it can be put, the persons to whom it can be disseminated, the right of inspection and expungement by citizens who might be affected by such information, and penalties for those who misuse such information. This legislation will be the subject of hearings and much study within the Judiciary Committee and I am confident that differences between the two bills which are today being introduced will be reconciled. I look forward to continuing my participation in this process.

SUBMISSION OF SENATE RESOLUTION 276—DISAPPROVAL OF PRESIDENT'S PAY RECOMMENDATIONS

Mr. DOMINICK. Mr. President, last April, I joined with Senators COTTON, YOUNG, MCCLURE, HANSEN, HRUSKA, GURNEY, PERCY, BARTLETT, THURMOND, TAFT, CURTIS, BELLMON, BENNETT, FANNIN, AIKEN, ROTH, and TOWER in petitioning the President to hold in abeyance any salary increases recommended by the Commission on Executive, Legislative and Judicial Salaries through the remainder of calendar year 1973 and until the inflationary threat was sufficiently under control to justify increases throughout the economy.

I was gratified that salary increases were not proposed last year. The budget submitted to the Congress yesterday by the President, however, included a pay raise for some 2,800 top officials in the executive, legislative, and judicial branches presently earning $36,000 to $60,000. This would also increase the salaries of nearly 10,000 career Federal employees who are now at the $36,000-a-year level. This raise will automatically go into effect within 30 days unless Congress votes it down.

Since I am still of the opinion that it would be counterproductive to seek any increases in salaries while the Nation is seeking to stabilize its economic position both domestically and in the international community, I am today submitting a Senate resolution on behalf of myself and Senators MCCLURE, HANSEN, GURNEY, BARTLETT, THURMOND, CURTIS, ROTH, TAFT, TOWER, and HELMS, to disapprove the recommendations of the President for a pay raise.

Mr. President, with the prevailing energy crisis, rising unemployment, inflation, and the threat of a recession combining to force our Nation's citizens to tighten their belts, it seems inconsistent to grant raises of $9,000 or $10,000 over the next 3 years to top officials of the Federal Government whose present salaries individually are from three to five times what the average American family earns per year.

I am confident that my colleagues will take these facts into consideration and am hopeful that they disapprove these salary increases before expiration of the 30-day deadline.

After all, one of the inflationary pushes we have in this country is deficit spending which has been OK by Congress. To have us, as Members of Congress, go ahead from there, and then we take care of ourselves while we continue deficit spending, seems to me to be totally out of line.

Mr. ERVIN. Mr. President, will the Senator from Colorado yield?

Mr. DOMINICK. I am happy to yield to the Senator from North Carolina.

Mr. ERVIN. Mr. President, I would like to ask the Senator if he would add my name as a cosponsor of his resolution.

Mr. DOMINICK. I would be delighted to do so. Mr. President, I ask unanimous consent that the name of the Senator from North Carolina (Mr. ERVIN) be added as a cosponsor of the resolution.

The PRESIDING OFFICER (Mr. DOMENICI). Without objection, it is so ordered.

Mr. DOMINICK. Mr. President, because of the urgency of this matter, I send the resolution to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The resolution will be stated.

The assistant legislative clerk read as follows:

S. RES. 276

Resolution to disapprove pay recommendations of the President

Resolved, That the Senate disapproves the recommendations of the President submitted to the Congress during February, 1974, pursuant to section 225(h) of the Federal Salary Act of 1967, as amended, with respect to rates of pay transmitted to the Congress during February, 1974.

The PRESIDING OFFICER. Is there objection to the present consideration of the resolution?

Mr. HUGH SCOTT. Mr. President, I object.

The PRESIDING OFFICER. Objection is heard. The resolution will go over under the rule.

QUORUM CALL

Mr. ROBERT C. BYRD. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The second assistant legislative clerk proceeded to call the roll.

Mr. MANSFIELD. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

THE TRUCKERS' STRIKE

Mr. MCCLELLAN. Mr. President, I want to make a few comments about an intolerable situation that is developing across this Nation. As all will remember, during the second week in December 1973, independent truck drivers by the thousands engaged in a general strike to bring the commercial life of the country to a halt. Shots were fired. Windshields smashed. Commercial terminals and truck stops were systematically obstructed. Wholesale blocking of highways inconvenienced thousands of travelers. By all appearances, the strike was coordinated and organized.

At that time I was stunned that my own State of Arkansas had acquired the dubious distinction of hosting the most violent incident in the strike—the explosive destruction of a tractor-trailer in Widener, Ark. That incident was vividly reported in the Washington Star-News on Friday, December 14, 1973. I ask unanimous consent that this article be printed in the RECORD following my remarks.

The PRESIDING OFFICER. Without objection, it is so ordered.

(See exhibit 1.)

Mr. MCCLELLAN. Mr. President, it is now February and the whole pattern is starting again, including the gunfire, malicious violence and wholesale obstruction. I ask unanimous consent that two articles from the Washington Post of February 2, 1974, describing these events to date be printed in the RECORD, following these remarks.

The PRESIDING OFFICER. Without objection, it is so ordered.

(See exhibits 2 and 3.)

Mr. MCCLELLAN. This obstruction and violence, which has adready resulted in the death of at least one person, cannot be permitted to continue any longer or tolerated in the future.

Mr. President, is the Federal Government without the tools to deal with this situation? The answer is "No." The civil rights provisions in title 18 of the United States Code give more than ample power to the Department of Justice to act. Citizens of the United States have a constitutional right to travel safely from one